CAPSTONE REQUIREMENTS DOCUMENT

GLOBAL INFORMATION GRID (GIG)

CRD Executive Agent
Commander in Chief, Joint Forces Command
Attn: C4 Plans, Policy and Projects Division (J61)
DSN: 836-5782/5540
Commercial: 757-836-5782/5540

TABLE OF CONTENTS

[1] CRD posted on World Wide Web at http://www.jfcom.mil/gigcrd

CHAPTER I GENERAL DESCRIPTION OF OPERATIONAL CAPABILITY

A. Introduction

1. Background. The task of preparing the Global Information Grid (GIG) Capstone Requirements Document (CRD) was assigned to the United States Joint Forces Command (USJFCOM) by the Joint Requirements Oversight Council (JROC) under the sponsorship of the Joint Staff/Command, Control, Communications and Computer (C4) Systems Directorate (J6) and the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD[C3I]). JROC Memorandum 135-99 (JROCM 135-99) of 23 November 1999 outlined the task for the development of this CRD. This document is the culmination of multiple strategy meetings and coordination initiatives that have occurred since 23 November 1999. The CRD development process was assisted by representatives from other Commanders in Chief (CINCs), Services, and Agencies, who participated in the GIG requirements development conference held 4 – 6 April 2000, and who provided input during subsequent document review and comment phases.

   a. The organization and content of this CRD are in accordance with *CJCSI 3170.01A Requirements Generation System* document dated 10 August 1999. It is also consistent with:

      - Chairman, Joint Chiefs of Staff's GIG Vision
      - OASD(C3I) GIG Systems Reference Model
      - Department of Defense (DoD) Chief Information Officer's (CIO) GIG definition (see paragraph A.2 below).

   b. The concept of a "Global Information Grid" was born out of concerns regarding interoperability and end-to-end integration of automated information systems. Issues such as streamlined management and the improvement of information infrastructure investment have also contributed to the heightened interest in the GIG. The real demand for a GIG is driven by the requirement for information superiority and decision superiority expressed in Joint Vision 2020 (JV 2020).

2. GIG Definition. A DoD CIO memorandum, dated 22 September 1999 and revised on 12 January 2001, by agreement by the DoD CIO, Under Secretary of Defense (USD) for Acquisition Technology and Logistics (AT&L), and the Joint Staff/J6, defines the GIG as follows:

   a. Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as

defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

b. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services (see paragraph c below with respect to embedded information technology).
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data or information for use by other equipment, software, and services.

c. The embedded information technology within a product is not considered part of the GIG; however, if it provides the functionality described in paragraph b above, it must meet GIG interface criteria. This is illustrated in Figure 1 below:

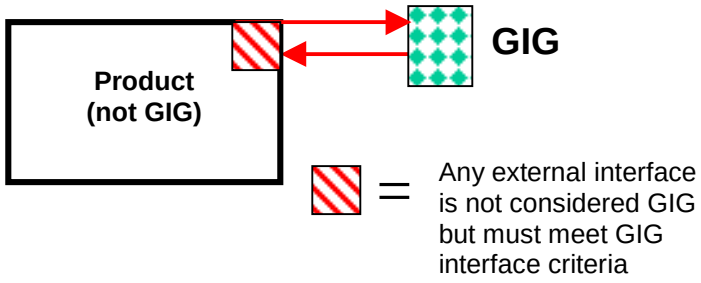


Figure 1. GIG Interface Criteria

3. Purpose. The purpose of this CRD is to describe the overarching information capability requirements for a globally interconnected, end-to-end, interoperable, secured system of systems that will support the National Command Authority (NCA), warfighters, DoD personnel, IC, policy makers, and non-DoD users at all levels involved in both military and nonmilitary operations.

4. Applicability. The capability requirements and the Key Performance Parameters (KPP) (including the information exchange requirements and the interoperability

KPP) outlined in this CRD will guide all DoD and IC components in developing Operational Requirements Documents (ORDs) for new systems and for upgrading legacy systems. This CRD will guide future Information Technology (IT) investments to ensure interoperability. All Mission Need Statements (MNSs), ORDs, or CRDs that are associated with GIG-enabled systems,[2] regardless of acquisition category (ACAT), must show compliance with this CRD, as appropriate/applicable.

5. Scope. The GIG is a system of systems that provides a set of value-added functions operating in a global context to support processing, storage, and transport of information; human-GIG interaction; network management; information dissemination management; and information assurance. These functions are fully interrelated, integrated, and interoperable with one another in order to achieve overall interoperability across the GIG. As a result, the GIG is an information environment comprised of interoperable computing and communication components.

B. Mission Area Description

1. Summary of Mission Need**.** A formal MNS for the GIG does not exist. Nevertheless, the need for the GIG has been documented in a number of reference publications, such as *Joint Publication JP 6-0* and *JV 2020,* and it has also been documented in a number of published MNSs, ORDs, and CRDs (e.g., Defense Information Systems Network CRD, Global Broadcast Service ORD, Information Dissemination Management CRD, Joint Tactical Radio System ORD, Global Combat Support System CRD, Theater Air and Missile Defense CRD, Warfighter Information Network – Tactical ORD, Joint Network Management System ORD, and Combat Identification CRD).

2. The GIG is essential for information and decision superiority. It will enable C4I integration of joint forces, improve interoperability of systems, and increase optimization of bandwidth capacity thereby dramatically improving the warfighting capabilities of joint forces across the full spectrum of conflict. The GIG will enhance operational capabilities while providing a common operational environment for conventional and nuclear command and control (C2), combat support, combat service support, intelligence, and business functions. In particular, the GIG will support:

[2] Any system that exchanges and/or disseminates information in the manner described in the GIG definition, and is in compliance with the capability requirements stated in the GIG CRD, as appropriate and necessary to fulfill the system's operational purpose(s)/mission(s), is considered to be GIG-enabled.

- Warfighters' ability to operate with reduced forces at high operational tempos where dynamic planning and redirection of assets is the norm.
- Delivery of information concerning targets, movement of forces, condition of equipment, levels of supplies, and disposition of assets to joint commanders, their forces, and the National Command Authority within required time frames.
- Warfighters' ability to obtain and use combat and administrative support information from national and widely dispersed assets.
- Collection, processing, storage, distribution, and display of information horizontally and vertically throughout organizational structures across the battlespace.
- Rapid and seamless flow and exchange of information around the globe to enable collaborative mission planning and execution from widely dispersed locations and at different levels (to include strategic, operational, tactical, and business).
- Timely, assured connectivity and information availability for decision makers and their advisors to support effective decision making.
- Integrated, survivable, and enduring communications for the NCA, Integrated Tactical Warning and Attack Assessment (ITW/AA), and strategic forces.

3. Related documents. There are currently no approved CRDs or ORDs, which pertain exclusively to the required capabilities described in this CRD, except for the Information Dissemination Management (IDM) CRD (dated 22 January 2001) which focuses on the IDM function. However, there are numerous proposed, draft, and current requirements documents (such as those cited in paragraph B.1 above), that address GIG functionality in some fashion.

4. Possible implications for changes to joint doctrine. All doctrinal publications that refer either to information management or to any of the functions of the GIG (see section C below) may have to be updated in accordance with the capabilities outlined in this document.

C. GIG Functions

The functions that support information flow and exchange throughout the GIG are organized and defined as follows:

a. Computing

- Process Function: A specified sequence of operations performed on well-defined inputs to produce a specified output. Computer-based processing is typically used for manipulating data, information, and/or knowledge into the desired form to support decision making and other GIG functions.

- Store Function: The retention, organization, and disposition of data, information, and/or knowledge to facilitate information sharing and retrieval.

b. Communications

- Transport Function: End-to-end movement of data, information, and/or knowledge between users and producers through other intermediate GIG entities.

c. Presentation

- Human-GIG Interaction (HGI) Function: The input and output of information representations between human(s)-in-control and GIG entry point(s).

d. Network Operations

Network Operations is an organizational and procedural framework for integrating Network Management (NM), Information Dissemination Management (IDM) and Information Assurance (IA).

- Network Management (NM) Function: The capability to monitor, control and ensure the visibility of the various networking and internetworking components.
- Information Dissemination Management (IDM) Function: Capability achieved through the use of a Family of Applications, Processes, and Services (FoAPS) to provide awareness, access, and delivery of information by the most effective and efficient means in a manner consistent with a commander's policy. It includes the following services:
  - Awareness: Information awareness services allow warfighters and other DoD users of information to discover what information is available both inside and outside of their respective communities and to determine what information has changed.
  - Access: Information access services allow warfighters and other DoD users of information to state their information needs and access information without being aware of the details involved in the retrieval process.
  - Delivery: Information delivery services optimize the use of infrastructure resources in accordance with the requested service and the commander's policy in effect.
  - Support: IDM support services provide the necessary interfaces to other GIG functions (e.g., store, information assurance, network management, etc.) to enable information awareness, access, and delivery.
- Information Assurance (IA) Function: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating

protection, detection, and reaction capabilities (*Joint Publication 3-13 Information Operations*).

D. GIG Operational Concept

1. The basic operational concept of the GIG is that warfighters and other authorized users in the DoD and IC, at any time and anywhere, can plug into the GIG and satisfy their validated user information requirements. From a logical perspective, the operational vision of the GIG is to facilitate interoperability among the fundamental building blocks, i.e., the operational elements of the existing IT infrastructure. By integrating disparate systems and networks into a unified global system, the GIG will empower warfighters with both information and decision superiority in every situation. As a caution, while the GIG holds promise for greatly enhanced information capabilities for all users, future developers must realize that resources, including bandwidth, are finite.

2. As a system of systems designed to foster integration, collaboration, and interoperability, the GIG is envisioned as a key enabler of information and decision superiority. It provides high quality, adaptive, and scalable information capabilities to meet, dynamically, the changing information needs of a warfighter.

3. The GIG will support DoD and IC information requirements and allow warfighters and other authorized users to process, store, transport, and use information regardless of technology, organization, or location. U.S. forces will have “plug and play” interoperability, while allied and coalition partners will be afforded connectivity on an as needed basis. The GIG will enable all warfighters to receive near real-time, fused battlespace situational awareness. It will allow commanders and their staff at the CINC, Joint Task Force (JTF), and Service Component levels to analyze data, anticipate requirements, focus on answers, and make real-time decisions rather than relying on historical information from multiple stovepiped automated information systems applications. Finally, the GIG will provide commanders with the environment needed to support information flow and exchange to accomplish missions collaboratively, simultaneously, and interactively, resulting in more efficient and substantially reduced operational decision making times.

4. Figure 2 depicts a high-level operational view of the GIG. It shows the organization of the logical GIG functions and their interrelationships, which are internal to the GIG. Also included in the operational view are the entities (e.g. allied, coalition, and other external) that reside in the environment external to the GIG. The GIG is required to interface with these external entities when engaged in the exchange and dissemination of information with them. From the perspective of those entities, the GIG is a virtual unified system of systems that interacts with them as a whole.

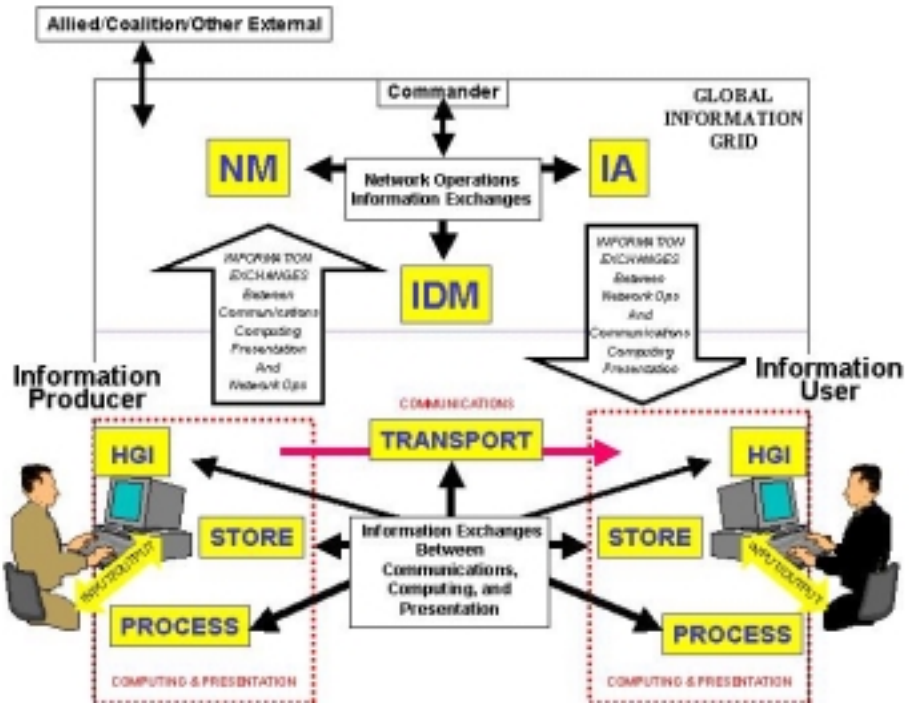


Figure 2. High-Level Operational View (OV-1)

5. The dynamic nature of information flowing across the GIG, and the time constraints within which information must often be delivered, require a new paradigm for characterizing and categorizing information. This new paradigm is based on the recognition that the first decision warriors must make regarding a piece of information is whether it requires them to take immediate action. The IDM function of the GIG will drive the dissemination of extremely time-critical information to those users who need it by matching the time-critical information elements with specific users. For these users, the identified time-critical information elements are called “survival” information because they convey one of the following three basic factors:

   - information that requires the recipient to take immediate action to avoid danger or hostile action
   - information that is essential to enable the recipient to take immediate action to destroy, nullify, or defeat a hostile entity, weapon, or force
   - information that will prevent the recipient from causing fratricide

6. The concept of survival information can be described as follows:

   - It is a subset of the information required for battlespace situational awareness. This implies that all survival information is relevant to situational awareness (SA). However, not all information used for SA can be considered as survival information.

- It pertains to perceived threats in the area of operations that are geospatially related to the individual warfighter or the fighting platform. Hence it informs about objects and events in the immediate geospatial region around a warfighter that can cause destruction of life and property.
- It is of short duration and prompts either an immediate action or a decision from the recipient.
- Survival information is also dependent on the context determined by current mission, operating environment, and commander's intent.
- Survival information is generally predetermined by the user on the basis of perceived threats.
- It is unique and distinct to each individual, process, and fighting platform in the battlespace. This implies that the same information element can be treated as survival information for one warfighter and as planning for another.
- It is required by individual warfighters and fighting platforms in real time or near real time. For survival information, near real time latency cannot exceed a certain timeliness factor of "n" seconds (see Survival Information Dissemination KPP[3] in Chapter IV.B.5.b) when the information is traveling from the exit point of B to F along the information delivery path as shown in Figure 3. In the path model, B is the first processor utilized that identifies an information element as survival information and designates the associated recipient(s). F is the final human recipient of the processed survival information. It should be noted that the processing time at B is being excluded, whereas any processing beyond B is included in the specified time frame.

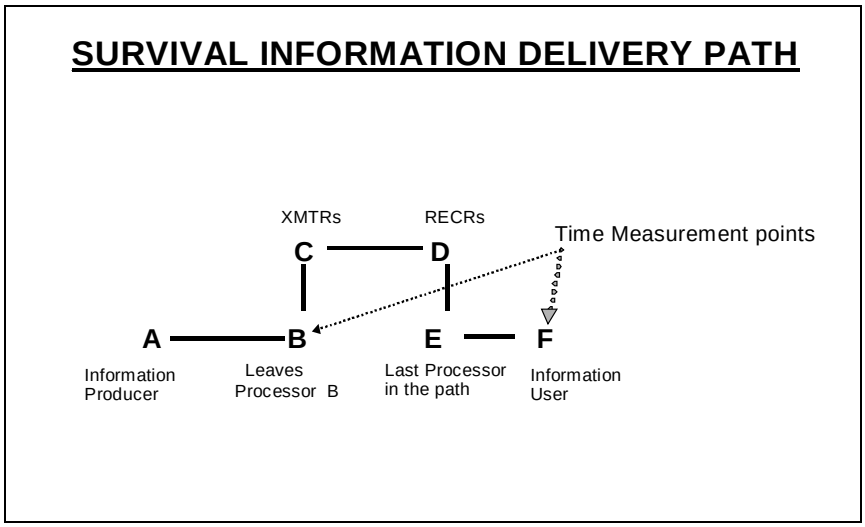


Figure 3. Information Path from Producer to User

[3] The Joint Requirements Panel (JRP) has forwarded the Survival Information Dissemination KPP (with Threshold/Objective metrics) to the Joint Requirements Board (JRB) as part of the Joint Requirements Oversight Council (JROC) approval process.

7. The paradigm also addresses the requirements of the majority of users and information elements that do not meet the above described survival criteria. For these users, information is characterized as ”planning” information because, even though in some cases it can be time sensitive, it is used to support some action in the future (including the near future). While it is true that some planning information requires time-sensitive dissemination for some users, it still does not meet the life-threatening time-critical survival requirements. Although this CRD does not attempt to subcategorize planning information into various delivery timeliness groupings, it is fully understood and accepted that specific Service or system ORD requirements may require further definition and/or categorization of planning information into distinct levels. To this end, multiple levels of planning information delivery requirements may be specified within an ORD.

8. Even though some information may be very time sensitive, if it does not meet the survival criteria listed above, it will be characterized as planning information. Generally, planning information is not as time sensitive as survival information. It is usually used for determining a future course of action and deliverable within the time limits specified by a user. When requesting planning information, users typically will either rely on the best efforts of the delivery system or may choose to specify an upper limit for information delivery time. Depending on user needs, the specified time limit for planning information can range from several seconds to hours or days.

9. The concept of survival and planning information is depicted graphically in Figure 4, where the threat is an incoming Scud missile. There are two users who would need the information on the incoming Scud delivered as survival information in “n” seconds[4] or less (Threshold). The Division Headquarters, as the probable target, needs to receive the information to prevent or reduce damage to itself from the impact of the Scud, and the Patriot Battery needs the information to engage the Scud and attempt to destroy it in flight. The third user shown in Figure 4, the afloat Battle Group, would need the same information delivered as planning information, so that it can take the Scud launch into account when planning future actions. Note that transmissions of survival information are typically short, bursty, and require minimal processing by the recipient.

[4] See Chapter IV.B.5.b. for Survival Information Dissemination KPP metrics. The Joint Requirements Panel (JRP) has forwarded the Survival Information Dissemination KPP (with Threshold/Objective metrics) to the Joint Requirements Board (JRB) as part of the Joint Requirements Oversight Council (JROC) approval process.

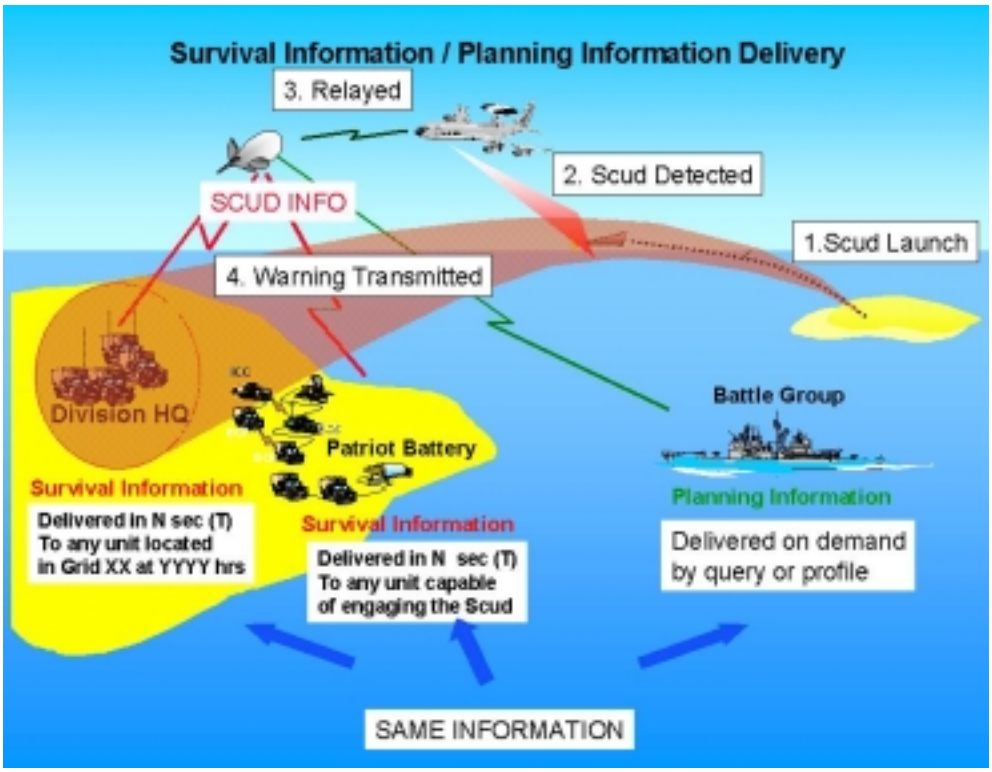


Figure 4. Survival / Planning Information Example

10. As shown in Figure 4, categorization of information as survival or planning will change depending on the operational situation, including both geographic location and operational mission of the information user. Therefore, it is the context that determines whether a particular information element meets the survival or planning criteria. Under predefined circumstances, certain information elements meeting the survival criteria for identified users, and thus requiring real-time delivery, must be disseminated to those users based on either an automatic response to a user profile or a manual response to a user query. In either case, once an information producer determines that information needed is of a survival nature, the information is then "pushed" for delivery. Such information elements requiring real-time delivery to designated user(s) are classified as survival information for those users. Non-time critical information elements that can either be "pulled" on demand through the query of stored data using a search mechanism, or be periodically "pushed" to a user based on that user's profile, are classified as planning information. It is also possible for information to be survival information for one user and planning information for another. This classification is determined by the time needed for the recipient to make a decision based on the received information.

E. Operational Suitability and Infrastructure Support

1. Operational suitability is the degree to which GIG systems can be satisfactorily developed, fielded, deployed, operated, and sustained while meeting performance parameters and the users' needs. The existence of global applications and systems such as the Global Combat Support System (GCSS),

Global Command and Control System (GCCS), Joint Network Management System (JNMS), and Defense Information Systems Network (DISN) will help operationalize the GIG, whereas existing stovepiped and legacy systems will impede its implementation.

2. The following guidelines are provided to help in implementing the GIG.

   a. The GIG should be implemented in accordance with the standards included in the most current version of the *DoD Joint Technical Architecture (JTA)*.

   b. All new Command, Control, Communications, Computers and Intelligence (C4I) emerging systems and upgrades should be fielded as Defense Information Infrastructure (DII) Common Operating Environment (COE) Level 6 compliant, with the goal of achieving Level 8 compliance.

   c. GIG-enabled systems should be either standards based or commercial-off-the-shelf (COTS) technologies that will:

      - Facilitate joint, allied, and coalition interoperability
      - Simplify integration
      - Reduce both long- and short-term costs

   d. Government-off-the-shelf (GOTS) and proprietary technologies should be used only if standards-based and COTS technologies are proven to be inadequate.

   e. All GIG-enabled systems should be scalable, affordable, sustainable, and extensible with respect to their functionality.

   f. All GIG-enabled systems should be designed to accommodate change and should facilitate the integration of future systems and technologies as they evolve.

   g. GIG-enabled systems should be consistent with the current DoD, IC, and commercial efforts regarding data and metadata standardization.

   h. All GIG-enabled applications should be designed to reside on current or proposed DII COE compliant systems, except where the requirement is waived.

   i. The goal and expectation of proposed GIG-enabled systems should be to minimize additional manpower requirements.

   j. The reliability, availability, survivability, and maintainability features of GIG-enabled systems should be designed to support all functions necessary to meet the requirements documented in chapter IV, including the ability to recover from critical failures.

   k. All GIG-enabled systems should be fielded with an emphasis on reducing the complexity, time, and cost of training. User training concepts should incorporate embedded training capabilities to the maximum extent feasible. In addition to being cost effective, human-machine interface design must be consistent with the capabilities and limitations of operators and support

personnel. Human-computer interface should also be designed to ensure quick and accurate information manipulation and assimilation. The utilization of existing installations and facilities for user training and support should be maximized.

l. Support functions and equipment should be consistent with operational requirements outlined in this CRD. Furthermore, software design should enhance interoperability and commonality within the GIG-enabled systems.

m. GIG-enabled systems should adhere to open system standards.

n. Bandwidth and throughput requirements along with implications to strategic, fixed, theater, and tactical architectures should be considered during the ORD and C4I Support Plan development process.

o. National Imagery and Mapping Agency (NIMA) standard military data should be used, where possible, to support common operational displays of geopolitical boundaries among the commands. Common operational displays should also be compatible with North Atlantic Treaty Organization (NATO) standards, as appropriate.

p. All GIG-enabled systems should be developed, tested, and deployed in a manner that is compliant with all appropriate treaties and international agreements.

q. GIG-enabled systems should be tested and certified for interoperability IAW Joint Interoperability Test Command (JITC) procedures.

r. Where applicable, GIG-enabled systems should enable users to operate in a multilingual environment to overcome the inherent language barriers of multinational and coalition operations.

s. GIG capabilities may require a re-evaluation of existing security measures currently in place. However, GIG-enabled systems and associated applications, processes, and services should not result in increased security risks and should meet all current security provisions articulated in appropriate DoD and IC policies, procedures, and instructions, including DoDD 8500.aa, Information Assurance. In particular, GIG-enabled systems should use standards-based rather than system-unique security mechanisms.

t. ORD writers should consider ongoing developments and evolving specifications in the following areas (as applicable):

- Joint Operational Architecture (JOA)
- Nuclear C2 Systems Technical Performance Criteria (NTPC)
- GIG Architecture

u. A checklist is provided in Chapter IV, Section D to facilitate ORD/CRD authors' compliance with this CRD as appropriate/applicable.

CHAPTER II THREAT

A. General

1. A detailed discussion of the foreign threat to the GIG does not exist. However, GIG-related threats are addressed in several DIA-validated, published documents: *Automated Information Systems Threat Environment Description (TED)* (U), NAIC-1574-0210-00, Sep 00, (S/NF); *Military Satellite Communications (MILSATCOM) Systems Threat Assessment Report (STAR)*, NAIC-1574-0367-00, Oct 00, (S/NF); *Electronic Warfare Threat Environment Description (TED)* (U), NAIC-1574-0731-01, Oct 00, (S/NF); and *Worldwide: Threats to Network Centric Warfare* (U), ONI-1573-001-00, October 1999 (S/NF). Additional relevant DIA documents to be published during 1-2QFY01 include: *Information Operations Threat to the Defense Information Systems Network (DISN)* (U), *Information Operations Threat to the Military Use of Commercial Satellite Communications* (U), *Information Operations Threat to the Secret Internet Protocol Network (SIPRNET)* (U), and a National Intelligence Estimate on the Cyber Threat to the U.S. The President's Commission on Critical Infrastructure Protection published its findings in October 1997. This unclassified document discusses the threat to the U.S. critical infrastructure, including telecommunications; electrical power systems; gas and oil production, storage and transportation; banking and finance; transportation; water supply systems; and emergency services. This chapter focuses the threat discussion on the information technology (IT) concerns of the GIG.

2. Threats to Critical Infrastructure. Many adversaries believe the best way to avoid, deter, or offset U.S. military superiority is to develop capabilities that threaten the U.S. homeland. In addition, our national infrastructure is vulnerable to disruptions by physical and computer attack. The interdependent nature of the infrastructure creates even more of a vulnerability. Foreign states have the potential capability to attack the GIG infrastructure. They possess the intelligence assets to assess and analyze infrastructure vulnerabilities, and a wide range of weapons conventional munitions, weapons of mass destruction (WMD), and information operations tools to take advantage of those perceived vulnerabilities.

3. The most immediate and serious infrastructure threats are from trusted insiders, terrorists, criminals, and other groups or individuals who are positioned to conduct well-coordinated strikes against selected critical nodes. While conventional munitions attacks are most likely now, over time our adversaries will develop an increased capacity, and willingness to employ WMD. They are also likely to enhance their capabilities for computer intrusion. COTS products and seamless services present new security challenges and concerns, providing opportunities to develop software functions that allow unauthorized access, theft and manipulation of data, and denial of service.

4. Skilled adversaries may be able to conduct pre-attack exploitation and attack preparations with nearly undetectable signatures, thereby minimizing indications and warning of their intentions. Any potential adversary is apt to target specific

information about the GIG in order to exploit or disrupt its operations. An adversary may target specific interconnections around the world, its end-to-end set of information capabilities, or the GIG's associated processes and personnel.

5. Threats to allies may become a threat to the GIG, even though the GIG may not be the primary target. Connectivity and interoperability with coalition, allied and non-DoD users and systems suggests an expanding universe of potential insider threats to consider. Because the GIG uses commercially available systems, widely available attack tools are becoming increasingly capable and deployable by people with fewer technical skills than previously required. One may expect adversaries to develop asymmetric responses to perceived vulnerabilities.

6. One form of asymmetric warfare to be considered is information operations (IO). Potential state-level adversaries could use IO tactics to enable military advantage, political and/or financial gain, and/or damage. Increased challenge, status, and/or thrills may motivate foreign non-state actors, such as hackers, to intrude into GIG systems. Evidence suggests that a successful attack against the GIG must be narrowly focused and precisely coordinated. Disrupting the entire GIG for an extended period of time is an unlikely event. In addition to IO, chemical and biological warfare threats are an expanding asymmetric threat to GIG operations. More information on these threats is contained in *Proliferation of Nuclear, Biological, and Chemical Weapons and Ballistic Missiles: A Primer* (U), DI-1569-20-99, December 1999 (S/NF).

B. Information Operations Threat

1. The primary threat tactic to the GIG comes from the information operations (IO) threat. Supported by intelligence exploitation, the IO threat includes the following tactics: computer network attack (CNA), computer network exploitation (CNE), electronic warfare (EW), radio frequency (RF) weapons, perception management, and physical attack.

2. Adversaries recognize our civilian and military reliance on advanced information technologies and systems, and understand that information superiority provides the United States with unique advantages. Many also assess that the real motivation for U.S. military actions is U.S. public opinion. Accordingly, potential foes could pursue IO capabilities as a relatively low-cost means to undermine public and political support for U.S. actions, attack key U.S. capabilities, and counter U.S. military superiority.

3. The IO threat continues to spread worldwide, with more mature technologies and more sophisticated tools being developed continuously. However, the level of threat varies widely from adversary to adversary. Most opponents currently lack the foresight or the capability to fully integrate all IO tools into a comprehensive attack. Many, with limited resources, will seek to develop only CNA options relying on modest training, computer hardware and software purchases, and/or the use of "hired" criminal hackers. At present, many nations have programs to protect their own information systems, and some, particularly Russia and China, are believed to have offensive information operations capabilities.

4. DoD systems are regularly probed and scanned, necessary activities before exploitation and/or attack, via foreign locations in order to define network architectures and assess vulnerabilities. Intelligence exploitation of the GIG can occur easily from various sources. Technical collection and analysis may provide adequate pre-attack information, such as data flow analysis and GIG architectural details. Technical collection tools are widely available and increasingly user friendly.

5. CNA and CNE tactics can be used against the GIG's computer systems, operating systems, and software applications. CNA and CNE include stealing passwords and data, inserting malicious code, denial of service (DOS), and data corruption, modification, and manipulation. The well-publicized distributed DOS attacks against several U.S.-based commercial Websites have sensitized foreign countries to their own vulnerabilities against this type of attack. Evidence suggests that some foreign entities have used DOS tactics against the GIG and introduced malicious code into the GIG.

6. EW tactics can be used against the GIG's wireless segments. Few commercial products provide electronic protect (EP) technology that could provide some defense against electronic attack (EA) and electronic support (ES) tactics. The rapid global growth of commercially available wireless communications systems has caused some countries to be interested in developing EW tactics against those systems, not necessarily against the United States. However, when common systems are used, then foreign EW may impact U.S. systems.

7. RF weapons, such as electromagnetic pulse (EMP) and directed energy weapons (DEW) can be used to physically disrupt electronic circuits. Foreign interest in protecting their own systems against these weapons can lead to increased understanding of the capabilities of RF weapons.

8. Perception management and physical attack may be used against GIG personnel and facilities, especially those portions controlled by foreign personnel in host nations.

C. Future Threat Trends

1. As DoD increasingly uses COTS technology and systems, the threat to unprotected systems will continue to grow. However, a primary impetus behind the globalization of information technology is electronic commerce, which will require improved information security (INFOSEC). Therefore, DoD may benefit from the global need for improved INFOSEC to enable personal privacy in electronic commerce and banking.

2. CNA/CNE tools will continue to grow in capability while the required level of user experience and knowledge to use them effectively decreases. These tools will become increasingly available on the Internet. Additionally, we expect to see more automated tools, such as the distributed DOS tools that use hundreds or thousands of previously exploited computers in a coordinated attack. Implementing the Defense-in-Depth strategy will minimize the reaction time to these emerging threats. Continued efforts will be needed to support Computer

Network Defense (CND) efforts to reduce vulnerability to the increasing potential threats. Defensive IO ensures the necessary protection and defense of information and information systems upon which joint forces depend to conduct operations and achieve objectives.

3. EW systems, especially ES systems, will continue to be produced, marketed, and exported around the world. As U.S. and global use of digital wireless networks grows, expect continued interest in intercepting and exploiting these systems. Some systems that are being marketed for law enforcement applications also have potential military use. Foreign critical infrastructure protection against RF weapon threats will continue to expand.

CHAPTER III SHORTCOMINGS IN MISSION AREA AND EXISTING SYSTEMS

A. General

1. Timely, relevant, consistent and accurate information is a fundamental requirement of the military decision making process. We face many challenges meeting this basic requirement, to include the use of multiple information formats, non-interconnected communications systems, and the absence of a common cataloging scheme for indexing information. Furthermore, some currently fielded information systems may not support the robust, assured, and timely flow of accurate and relevant information needed to meet future joint warfighting needs. In addition, operational fragmentation and segregation of information by type, classification, command, and mission make it difficult to transport, store, and process essential information across/within the Joint Task Force. The information flow problems are especially critical with our allied and coalition partners.

2. Information needed by the military and the capabilities to provide that information are undergoing a revolutionary transformation. Global communications, data storage capacity, transmission speeds, information availability, and resulting bandwidth demands are all growing exponentially. However, our need for timely and precise information also continues to grow at a tremendous rate. Improvements in information technology and the evolution of commercial and IT standards have outpaced our processes and tools for managing information and its dissemination. Search and retrieval capabilities are hampered by the lack of a common data standard. Finding and accessing specific information can be a time consuming and involved process due to the differences in naming conventions and lack of associated semantics. Furthermore, due to the lack of a precise retrieval capability, the volume of information retrieved from a single query can be excessive, requiring the users to spend valuable time sorting through large amounts of irrelevant or duplicative data. Transmission of such excessive data also unnecessarily consumes throughput capacity. Retrieved information may also come from stovepiped sources that are not interoperable, thus making it difficult/impossible for the receiving system to use it (e.g. to merge the received information into a common operational picture). Additionally, the lack of a dynamic capability to monitor and control bandwidth utilization greatly inhibits a commander's ability to make timely resource reallocation decisions. Finally, while new systems are providing a tremendous increase in information availability, the commonality or interfaces to permit the cross-flow of this information among the systems are inadequate. The results are wasted capacity, increased redundancy, decreased interoperability, incompatible standards and formats, and reduced cross-functional and/or organizational information flow.

3. Fielding new information technology (IT), especially in a networked environment, is a complicated and challenging endeavor for both the mission application users and IT support staff. Security vulnerabilities in one system impact all connected

systems and could allow access and sabotage of other interacting systems. The lack of proper integration with existing systems and/or viable logistics support to include life-cycle maintenance and ongoing training can quickly erode the capabilities of the IT systems.

B. Computing

1. Process

a. Current information systems cannot support warfighter requirements for distributed processing due to interoperability and security limitations. This situation particularly impacts dispersed operations, such as wide-area air and missile defense, where a coordinated operational picture and weapons employment is essential.

b. Collaborative processing capabilities are very limited, which in turn, limits the ability of commanders and their dispersed components to plan efficient operations.

c. There is a lack of interoperable applications, which directly impacts coordinated planning, collaboration, and operational execution across the battlespace.

2. Store

a. Users and producers cannot rapidly index/catalog, store, search, and retrieve required information. This shortfall constrains the commander's decision-making ability because essential accurate information is not available in a timely manner to facilitate decision superiority.

b. Currently, DoD does not have a prescribed storage standard that would provide the optimum capability across DoD to store, search, and retrieve data in an expedient time frame with appropriate quality or the ability to identify associated information. Therefore, commanders at all levels are unable to acquire essential information from data repositories on which to base operational and tactical decisions. This capability is essential to achieve decision superiority.

C. Communications

Transport

a. We cannot effectively and efficiently use the existing available RF spectrum. This situation further exacerbates the current bandwidth shortage resulting in a restricted ability to support the command decision process.

b. Bandwidth capacity is significantly limited across the strategic, operational, and tactical levels. Solutions exist for bandwidth problems at the strategic and, possibly, the operational levels through new technology (broadband initiatives), but at the tactical levels, this bandwidth shortage is expected to remain into the foreseeable future. Current disparities between bandwidth needs and available capacity lead to warfighters not training as they will fight.

c. The ability to move digital information seamlessly is reduced by the current use of proprietary protocols and a lack of prescribed DoD transport standards. This constricts the flow of essential information to commanders and weapons systems thus impeding time sensitive operations across the battlespace.

d. Current DISN communications infrastructure (e.g. Non-secure Internet Protocol Routing Network – NIPRNET and Secure Internet Protocol Routing Network - SIPRNET) does not meet many of the GIG requirements for quality of service (QoS), bandwidth availability, and transmission priority management; thus the DISN must be enhanced to meet these stated requirements. This shortcoming greatly impedes the exchange of both unclassified and classified information across the GIG to meet warfighter requirements.

D. Presentation

1. Human-GIG Interaction (HGI)

a. The ability to present information to the human user is reduced by the heavy reliance on the use of text message formats and the inability to provide multimedia presentations. Computer systems and devices are currently tailored to interface with only two human senses: sight and sound. This requirement to manually read voluminous textual material slows the decision-making process.

b. The inability to process multiple languages of both spoken language and applications limits the effective presentation of information. This situation is particularly constraining in allied and coalition operations, which constitute a vast majority of the operations involving the U.S. military today.

c. Systems lack the capability to ascertain the context in which humans are functioning, and thus provide information in a predetermined way rather than in the form most useful to the human given the role, mission, and function assigned. Lacking the ability to present information in the most effective and efficient manner for human use impedes military processes requiring human–system interaction.

d. Current systems are non-adaptive to user needs and cognitive styles. The systems are often non-intuitive in meeting the users' requirements and are not user friendly. Lack of this ability to present information in the most effective and efficient manner for human use slows all military processes requiring human–system interaction and has a direct effect on a commander's effective decision making ability.

e. There are no effective automated means for users to locally prioritize information inputs and flexibly control the ways and manner in which information is presented to them for review/alert. This limits an operator's ability to modify their information receipt and notification to correspond to the operational situation. There is also a possibility that in some cases, the

receipt of time-critical survival information could go unnoticed because of this shortfall.

E. Network Operations

1. Network Management (NM)

a. There is a lack of asset visibility resulting in an inability to effectively manage the overall network to support common user needs. The limited network visibility is significantly impacted by the large number of stovepiped and legacy systems. Stovepiped and legacy systems are normally not designed to support global, end-to-end network management or adhere to a prescribed set of standards for interoperable use across DoD and the Intelligence Community. However, there are dedicated/specialized systems that are required to accomplish specific command missions, but do not support or facilitate effective network management of these systems.

b. There are no common prescribed standards for common user systems/networks that would facilitate network management across DoD/IC. This shortfall precludes effective network management, which is essential to ensure the most efficient and effective exchange of information across the battlespace.

c. There is no distributed network management capability that would allow the management of common user networks from more than just one central location.

d. Existing network management is currently unable to provide a fully integrated multilevel security network.

e. DoD has little or no network management capability to accompany its increasingly widespread use and application of advanced mobile wireless computing and networking which are inherently ad hoc.

f. There is no prescribed standard joint network management capability for JTF component-level common user systems/networks. Deployed network management suffers from a loosely federated approach for employing GOTS and COTS software.

g. Current end-to-end communications, especially in the last tactical mile, are not fully integrated and interoperable. Specific issues include heterogeneous network design, inconsistent firewall implementations and varying network management policies and tools.

2. Information Dissemination Management (IDM)

a. Most military information systems are designed to support the collection, analysis, storage, and distribution of non-time-critical planning information instead of time-critical survival information. This can seriously impede the flow of survival information to those for whom it can mean life or death.

b. There is insufficient capability to produce and disseminate time-critical survival information to specific warfighters based on a set of static information

profiles, much less a set of situational dependent profiles. This can seriously impede the flow of survival information to those for whom it is critical based on their dynamically changing operational situation.

c. Users lack visibility to available information/data. This shortfall seriously restricts the ability of commanders and decision-makers at all levels to acquire information essential to making operational and tactical decisions. Having the right information at the right time and at the right place is essential for achieving decision superiority.

d. Producers cannot make information/data easily available to the user in a desired format. This causes users to spend precious time reformatting and converting received information, which has the overall effect of restricting the command decision-making process and can adversely affect the success of military operations. When decisions must be made in seconds, it is essential that information arrive in a format that a user can immediately utilize.

e. Users have a limited means to easily access information without prior knowledge of exact locations where the information is stored. This shortfall constrains the commander's decision-making ability, because essential accurate information is not available in a timely manner.

f. The commander has a limited ability to visualize the flow of information into and within his area of responsibility (AOR). Therefore, the commander has limited ability to inject guidance to dynamically adjust his communications infrastructure priorities with respect to a changing operational environment.

g. Users cannot easily create or dynamically adjust their user profiles to allow for better flow of information. Therefore, commanders are unable to adjust their information requirements to ensure the receipt of critical information. This is essential in today's warfighting environment where conditions are constantly changing.

h. Few automated means for prioritization of information/data exists to ensure that high priority information requests are handled first. This is particularly crucial to the delivery of survival information to designated users in critical tactical situations.

i. Current systems do not allow for the dynamic routing of information to the most efficient communications pathway available. Creating efficient communication pathways will ensure network optimization.

j. There is limited awareness of user information requirements due to inconsistent, non-interoperable, and antiquated methods of communicating these requirements to producers. This can greatly restrict the commanders' ability to acquire essential information in a timely manner.

k. There is limited status provided to users to provide visibility into the progress of satisfying their information requirements. Therefore, commanders and their subordinates lack the ability to forecast when key information might become available, if at all, to support critical military decisions.

l. Current U.S./NATO classification and security policy does not allow NATO classified information to move across U.S. classified systems.

3. Information Assurance (IA)

a. Currently there is very limited flexibility and adaptability of information security to support multilevel security operations, which can greatly impede effective command and control of military operations by restricting the availability of needed information to key decision-makers.

b. Available IA technology solutions are not capable of providing effective protection against the full range of potential cyber threats. This places at risk our entire command decision-support capability on which practically all military operations rely.

c. Information systems are vulnerable to passive intercept attacks, which include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing identification (ID) numbers and passwords. These efforts can give adversaries indications and warnings of impending actions.

d. Information systems and information content are inherently vulnerable to insider attacks by malicious authorized users, which can seriously compromise the command decision process at all levels by removing or constricting automated decision support capabilities. There is a lack of a capability to consistently access sensitive/classified information by cleared persons having the appropriate need to know and to transfer sensitive/classified information across networks running at different classification levels. Therefore, commanders at all levels are limited in their ability to acquire essential information from data repositories and to base operational and tactical decisions on that information.

CHAPTER IV CAPABILITIES REQUIRED

A. GIG Capability Requirements. This section describes GIG capability requirements. Capabilities are listed within seven fundamental functions (process, store, transport, human-GIG interaction, network management, information dissemination management, and information assurance), organized into four general categories (computing, communications, presentation and network operations). Because the GIG operates as a globally interconnected, end-to-end, interoperable system of systems, all systems that comprise the GIG shall be GIG-enabled so as to allow "plug and play" interoperability among systems. A system shall be considered GIG-enabled if it has the capabilities described in this chapter for the seven GIG functions, as appropriate and necessary to fulfill the system's operational purpose(s)/mission(s). The capability requirements under each functional area are shown in *italics*. A checklist is provided in Section D for ORD/CRD authors to complete a capability requirements crosswalk to ensure compliance with the GIG CRD as appropriate/applicable.

1. Computing: Process Function

   a. General. Although computer-based processing is inherently involved in the execution of all GIG functions, the requirements outlined in subparagraphs (b) through (w) below are biased toward computing processes used for manipulating data, information, and/or knowledge into the desired form to support decision making and other GIG-supported activities.

   b. Processing Efficiency and Effectiveness. The stated capability assumes that resources available for computing and dissemination are finite and constrained. This assumption holds true for all computing environments. Therefore, *all computing processes of systems shall optimize the use of constrained computing and dissemination resources* **(*Threshold*)**. Based on the specified requirements, process efficiency can be traded off with process effectiveness. If the marginal benefit of utilizing additional resources exceeds the cost of resources used, then effectiveness of processing should prevail on the process efficiency.

   c. Reuse of Information Products. *Systems' previously generated, shareable information products (i.e. processed data) shall be reused to maximize consistency and efficiency, and to minimize process redundancy* **(*Threshold*)**. Use of computing resources to reprocess raw data to regenerate information that is currently available and accessible within the GIG environment should be avoided. Besides being efficient, elimination of redundant processing promotes consistency in the processing of raw data.

   d. Processing Mode. *Systems shall have processes that accommodate an interactive and multimedia processing environment within the GIG* **(*Threshold*)**. *The need for other processing modes, especially batch processing, shall be clearly demonstrated prior to their adoption* **(*Threshold*)**.

Systems shall use time-critical processing when dealing with survival information in order to meet stringent timeliness requirements (***Threshold***).

e. Value-added Processing. *Systems shall have processes that add value to the information and that are deemed necessary as well as essential for the implementation of the target system* **(*Threshold*)**. Adding value implies that the output generated by the process shall be more meaningful for the task at hand when compared to the inputs. As a result, a process shall be considered relevant only if it is capable of making a positive contribution to the semantic content of the information or data being manipulated by it. Essentially, the characteristics of the information exiting the process shall be more useful or beneficial to its consumers than the characteristics of the information entering the process. Based on its value to the target system, a process shall be retained, standardized, eliminated, outsourced, consolidated, and/or reengineered.

f. Cohesiveness. *Each process of a system shall accomplish a well-defined, single function, so as to achieve cohesion and enhance process reusability and system maintainability* **(*Threshold*)**. Cohesiveness is an internal characteristic of process design and generally leads to modular and maintainable systems. It also promotes process reusability. Cohesion can range from low to high, where the low is characterized by coincidental cohesion and high is characterized by functional cohesion. On the low side, the tasks performed by a process are either very loosely related or may also be unrelated to one another. A high degree of cohesion implies that the process is performing one distinct procedural task.

g. Modularity. Non-modular processes are monolithic and complex. Hence, computing processes designed to be modular are typically small in size, simple to understand, exhibit high cohesiveness and use simple interfaces to interact with other processes. Simplified interfaces imply low coupling and lead to relatively independent processes. *Systems' processes shall be modular to reduce maintenance and promote reusability* **(*Threshold*)**. Modularity allows processes to be treated as "black boxes," which enables plug and play systems and operational architectures.

h. Process Reusability. *Systems shall have, to the maximum extent possible, processes that are designed (using off–the–shelf standard components built according to an open standard) and implemented to be reusable in multiple systems and computing environments as plug and play "commodities" or "generics" rather than custom built from scratch each time* **(*Threshold*)**.

i. Reliability. *Systems shall have processes that are classified either as deterministic or non-deterministic, with each deterministic process producing consistent and definite results, and each non-deterministic process specifying a range with boundary limits and the expected average for each output generated* **(*Threshold*)**.

j. Validation. *The accuracy of outputs from systems' processes, deterministic or otherwise, shall be testable, meaning that processes shall be executable*

and the actual outputs generated by a process shall conform to expected outputs governed by operational requirements **(*Threshold*)**. *In the case of system's non-deterministic processes, it shall also be possible to predict all outputs within specified limits* **(*Threshold*)**. The output limits used for validation will match the output limits specified for process reliability.

k. Verifiability. *Systems shall have processes that facilitate verification and verification activities shall be performed to discover design errors and demonstrate the conformity of the system to the specified requirements* **(*Threshold*)**. Conformance to the specified requirements establishes a traceable path from the designed and implemented system to the specified functionality of the system. This allows the system developer to demonstrate that the system is doing what it was specified to do. Since verification prevents system developers from building the wrong system, it is imperative that all processes facilitate verification activities. Verification and validation differ in their objectives. Verification is a check for building the system the right way regardless of whether it is the right system or not, whereas validation ensures that the right system was built. Verification is also instrumental in eliminating costly errors during early stages of the development process, which eventually results in reduced maintenance costs.

l. Interprocess Communications (IPC). *To achieve interoperability among systems' processes, all processes shall use standardized mechanisms to communicate with each other, and process interfaces shall follow established standards for interprocess communications regardless of whether they are communicating with processes residing within the same computing system or with processes residing on remote systems* **(*Threshold*)**. IPC standards shall be followed for all process to process communications, which include data exchange, service request, and remote invocation. Also, standards used by a process for interprocess communication shall not be dependent on the characteristics of the remote process. Similarly, it shall be a material consideration for IPC, whether the remote process is a part of a legacy system, resides within the GIG environment, or resides outside the GIG boundary.

m. Process Prioritization. *Systems' processes shall be responsive to task prioritization dynamically* **(*Threshold*)**. Computing processes that are common across multiple tasks shall be responsive to the priority attached to the task regardless of the mechanism used for establishing the task priority. It will be assumed that the task priorities can be changed dynamically and therefore the process shall also be capable of changing its response to task prioritization dynamically.

n. Process Adaptability. Processes shall not make any absolute assumptions about available computing and communication resources. *All critical processes of systems shall have the capability to monitor the available resources and dynamically adjust their processing characteristics and behavior in accordance with the resources made available for their use* **(*Threshold*)**.

o. Standards-Based Processing. *All processes of systems shall demonstrate compliance with existing directives, instructions, and prescribed standards* **(*Threshold*)**. When appropriate, decisions regarding the applicability of directives or instructions will be biased toward those most widely used directives and instructions in the GIG environment. In accordance with *Title 10 (Chapter 131)*, DoD CIO prescribed industry, international, Federal Information Processing Standards (FIPS), NATO STANAGS and MIL-STANDARDS will be used by the GIG.

p. Process Security. *All processes of systems shall be protected and secured at appropriate levels and be visible to and cooperate with all information assurance operations* **(*Threshold*)**. This implies that access to a process shall be controlled. Furthermore, only authenticated users will be allowed to access a process. The level of security associated with the process shall be appropriately justified. It will depend on the sensitivity of the task being accomplished by the process and governed by a formally established security policy.

q. Non-GIG Interoperability. If and when required, processes residing in the GIG environment shall be capable of interfacing with processes residing on non-GIG systems while retaining GIG security and integrity. *Systems' processing shall accommodate non-DoD* **(*Threshold*)** *and allied and coalition* **(*Objective*)** *operations when necessary.*

r. Robust and Flexible Processing. *All process failures and processing exceptions of systems shall be handled through error-handling and recovery mechanisms that are consistent with threat and risk levels associated with the processing task* **(*Threshold*)**.

s. Analytical and Collaboration Services. *Systems' processing shall support analytical and collaboration capabilities through services that support collaborative planning, decision making aids, modeling and simulation, data mining, intelligent agents, and virtual workspaces* **(*Threshold*).**

t. IM Support. *Systems' processing shall accommodate all Information Management (IM) tasks related to creation, acquisition, transmission, organization, storage, dissemination, presentation, protection, and disposition of information, as well as other information processing tasks guided by and in compliance with the DoD CIO IM Strategic Plan* **(Threshold)**.

u. Interface Definition. *All process interfaces of systems shall be well defined and clearly specified, to include at a minimum, all input specifications, output specifications, and specifications for controls required for triggering the process* **(*Threshold*)**.

v. Cross-Platform Functionality. *Systems' processes shall be independent of the computing platform regardless of the programming or scripting* **(*Threshold*)**.

w. Process Availability. *Systems' processing components shall ensure that the overall system availability is not compromised due to run-time process failures* **(*Threshold*)**.

2. Computing: Store Function

a. General. The store function is responsible for the retention, organization, and disposition of information to facilitate information sharing across the GIG.

b. Data Interoperability. *Systems shall identify and use common standards for data and metadata representation* **(*Threshold*)**. *All of a system's data that will be exchanged, or has the potential to be exchanged, shall be tagged IAW the current JTA standard for tagged data items (Extensible Markup Language [XML]), and tags will be registered in accordance with the DISA COE Data Registry, Level 6* **(*Threshold, KPP*)***/ Level 8* **(*Objective, KPP*)**. When a standard exists, the developer shall use the standard. In cases where standards do not exist for a class of data that is being stored, the developer shall be responsible for unambiguously defining both the syntax and semantics.

c. Data Integrity. *Systems' storage process shall not alter stored data in a manner that compromises the integrity of the data without the user's knowledge and consent* **(*Threshold*)**. Compression and other similar storage techniques shall be authorized as long as the information the user retrieves from the storage process has not been altered or changed from the information that was placed in storage.

d. Infrastructure Management. *Systems shall provide visibility of storage infrastructure to efficiently manage the available storage capacity and provide the capability to remove/discard/update stored data as required* **(*Threshold*)***.*

e. Data Distribution. *Systems' data shall be stored in a manner that facilitates its distribution IAW processing and transport needs and supports the rapid retrieval of the information by the user* **(*Threshold*)**. *Each item of stored data shall have a single, discrete source of reference, so that future updates of that data, while being stored in other locations, will be able to refer back to the designated single reference source, thus ensuring that the information is being updated with the most current available version* **(*Threshold*)**.

f. Data Survivability. *Systems' data shall be stored in a manner that assures the required access to and use of all needed data, and in a way that prevents the loss of stored data from physical threats such as fire, water damage, information operation threats, and Electromagnetic Pulse (EMP) as appropriate to the information being stored* **(*Threshold*)**.

g. Data Security. *Systems' data being stored shall include its classification and releasability criteria within the semantic tag or associated schema* **(*Threshold*)**.

h. Data Disposal. *Systems' data that is no longer required shall be disposed of effectively and efficiently, so that the storage space that was used by the*

disposed data can be used for the storage of new data without the user having to do any additional actions once the decision to dispose has been made **(*Threshold*)**.

i. Data Retention*. Systems' data shall be returned in a manner that meets all mission and regulatory guidance and is transparent to the user* **(*Threshold*)**. Short-term retention should meet operational needs of the warfighter and long-term retention should meet legal or other regulatory requirements.

3. Communications: Transport Function

a. General. Transport is the movement of information and/or knowledge among consumers, producers, and intermediate entities.

b. Switching/Routing/Transmission. *To ensure the unimpeded exchange of information that is necessary to meet user requirements, systems providing switching, routing, and transmission control capabilities/mechanisms shall be fully interoperable and work seamlessly across the entire GIG, in accordance with the DoD JTA* **(*Threshold*)**.

b. Spectrum Supportability/Electromagnetic Environmental Effects**.** *Systems shall optimize the use of the electromagnetic spectrum through efficient frequency reuse and advanced modulation, compression, and filtering techniques, and shall comply with DoD, National and International spectrum management policies as applicable* **(*Threshold*)**. *Systems shall be mutually compatible with other systems, including allied and coalition systems, in the operational environment and shall not be degraded by electromagnetic environmental effects* **(*Objective*)**. *Spectrum certification and an electromagnetic environmental effects limitations/vulnerabilities report shall be obtained for 95 percent of systems* **(*Threshold*)** *and 99 percent of systems* **(*Objective*)**.

d. Quality of Service (QoS). Emphasis on superior QoS commensurate with each user's requirements must be an overarching GIG operating principle. *Transport systems shall provide QoS capabilities that ensure information identified as priority is delivered ahead of regular traffic 99 percent of the time* **(*Threshold, KPP*)** *and ahead of regular traffic 99.9 percent of the time* **(*Objective, KPP*)**. Required QoS factors include:

- Prioritization. *End users shall be able to assign priority to information targeted for transport* **(*Threshold*)**.
- Response Time. *All transport capabilities shall be designed to meet or exceed customer stated response times* **(*Threshold*)**.
- Precedence. *Data shall receive expedited handling during transport in accordance with the commander's policy and user assigned priority* **(*Threshold*)**.
- Reliability. *Delivery of information shall be guaranteed in accordance with its assigned broadcast level* **(*Threshold*)**.

- Latency. *It shall be possible to deliver information in real and/or near real time* **(*Threshold*)**.

e. Information Integrity. *Transport systems shall maintain and guarantee during transport the integrity of all information elements exchanged throughout the GIG to enable user confidence; information integrity shall be 99.99 percent* **(*Threshold, KPP*)** *and 99.999 percent* **(*Objective, KPP*)**, as specified in the Information Dissemination Management (IDM) CRD as an information delivery requirement.

f. Standards. *To ensure system interoperability across the GIG and to support assured uninterrupted service, all transport capabilities shall be standards-based using DoD JTA and other DoD CIO prescribed standards, as applicable* **(*Threshold*).** It is only through the rigid enforcement of and compliance with such standards that fully GIG-wide information exchange shall be possible. Due to the number of variables involved, intelligent agents may be needed to negotiate particular aspects of the standards that are to be invoked.

g. Connectivity. *Transport systems shall provide connectivity on demand to all fixed and deployed locations/users* **(*Threshold*).** This on-demand, seamless connectivity is essential to satisfy the rapidly changing requirements of warfighters at all levels engaged in operations throughout the world. Unimpeded mobility, while maintaining uninterrupted connectivity both laterally and vertically are basic requirements of the 21st century warfighter. This is essential given the combination of a shrinking force structure and the ever-increasing missions and locations where our military forces are required to operate. *Transport systems shall have the ability to maintain network connectivity on-the-move to meet both Service and JTF requirements in all warfighting environments (afloat, sub-surface, airborne, in space, and on the ground)* **(*Objective*)**.

h. Capacity. *With minimal exceptions, GIG transport capacity shall be viewed as an open system that is available to transport information from all domains utilizing unicast, multicast, and broadcast techniques to provide information on demand to the warfighter/decision maker* **(*Threshold*).** *Transport systems shall have the reserve capacity to accommodate surge loading and support multiple military operations as described in Defense Planning Guidance* **(*Objective*)**.

i. Technology Insertion. To effectively keep pace with advances in technology that have the potential to render existing systems obsolete shortly following acquisition*, the GIG shall enable and support the seamless and efficient insertion and incorporation of emerging (future) technologies into the transport domain* **(*Threshold*)**. Such a technology insertion provision is essential to maintain the operational effectiveness of the GIG.

j. Security. *Systems shall provide link and transmission security based on the level of risk acceptable to the user, and the GIG security architecture shall support use of clear headers* **(*Threshold*)**.

k. Robustness. Transport system reliability is a fundamental requirement for ensuring necessary information exchanges to support military operations. A primary concern in any transport architecture is single points of failure. *To avoid any single point of failure, the GIG shall use multiple connectivity paths (not susceptible to the same threat) and media* **(*Threshold*)**.

l. Scalability. Modern military force deployment scenarios require varying force levels depending on the particular mission and associated operational requirements. Therefore, *transport capability shall be scalable and adaptable to meet the dynamic needs of users* **(*Threshold*)**.

m. Survivability. *Transport systems shall be protected against all potential threats commensurate with the operating environment and the criticality of the information being transported, and shall also ensure connectivity through the total threat environment (i.e., conventional and nuclear*) **(*Threshold*)**.

n. Availability/Reliability. *To be effective, transport capabilities shall be available to provide reliable information exchange services to the warfighter/decision maker on demand and shall be responsive to the criticality of the information to be exchanged* **(*Threshold*)**.

o. Tactical Deployability. Military tactical forces require maximum mobility and ease of deployment. This requires that their supporting systems also be easily transportable. Therefore, *transport systems supporting tactical forces shall minimize lift requirements and be transportable using existing JTF/Service notional lift capabilities* **(*Threshold*)**.

p. Transport Element Status. *All transport elements (e.g. switches, routers, etc.) shall be capable of providing status changes to network management devices by means of an automated capability* **(*Threshold/Objective, KPP*)**.

q. Secure Voice Interoperability. *Strategic secure voice systems and tactical secure voice systems shall be interoperable, with a 99%* **(*Threshold, KPP*)** *and 99.9%* **(*Objective, KPP*)** *call throughput success rate.* Throughput success/failure is defined as a call completion rate when both secure voice systems are operational and available.

r. Secure Voice with Allied and Coalition Forces. *Secure voice cryptography shall be provided to or developed with allied forces that enables interoperability* **(*Threshold*).** *Secure voice systems shall be interoperable with coalition forces* **(*Objective*)**. *A secure voice system shall be able to be provided to coalition forces that is interoperable with the U.S. version using coalition releasable technology* **(*Threshold*)**.

4. Presentation: Human-GIG Interaction (HGI) Function

a. General. HGI is the input and output of information representations between human(s)-in-control and GIG entry point(s). The system design will minimize human performance errors, interface problems, and workload (physical, cognitive, attention) requirements. Interface characteristics will be chosen to maximize human productivity and performance as verified by iterative testing.

Parametric thresholds and objectives for acceptable human performance shall be established in the MNSs, ORDs, and CRDs.

b. Output/Input. *Systems' HGI shall present information to the human using a combination of visual, aural, tactile, and/or other sensory methods* **(*Threshold*)**. Output requirements need to encompass new methods of output as well as more advanced graphical displays, animation, and immersive technologies such as virtual realities. Software download capabilities that provide basic user-assisted functionality such as metadata encoding, converters, fonts, rendering, and input method editors shall be available as needed.

- Visual Presentation. Visual methods shall be selected from the full spectrum of means, simple to complex, as suggested by blinking lights and plain text through full-motion, stereoscopic, color imagery and human visual inputs. Seventy percent of the body's sense receptors cluster in the eyes.
- Aural Presentation. Audio methods shall be selected from the full spectrum of means, simple to complex, as suggested by a single constant tone through multi-language, stereophonic, synthesized speech.
- Tactile Presentation. Tactile methods shall be selected from the full spectrum of means, simple to complex, as suggested by simple applications of pressure and/or vibration to complex patterns of pressure, temperature, and vibration.

c. Feedback. *Systems' HGI shall provide unobtrusive confirmations of user input and actions, to include implicit visual, aural, and/or tactile feedback in response to user actions (e.g., push-button highlighting, mouse button or keyboard key "clicks," or audible tone) as well as explicit notifications that entered data was properly entered, accepted by the system, and/or errors were detected* **(*Threshold*)**.

d. Specialized Environments. *System's HGI shall functionally accommodate use in an NBC or other specialized operating environment, as designated by mission needs* **(*Threshold*)**. Not all user interfaces will be required to operate in all possible operating environments. Other specialized environments may include cockpits, mobile environments (e.g., tanks), hand-held radios, ships, low light, etc.

e. Usability. *Systems' HGI shall be usable by all end-user skill levels in the aspects of learnability, flexibility, and tailorability, which shall be verified by iterative user testing* **(*Threshold*)**. Parametric thresholds and objectives shall be established by the ORD. Measures of effectiveness and measurable performance criteria shall be defined by determining system usability during user evaluation and tests.

- Learnability. Systems' HGI shall minimize the time and effort required to reach a specified level of user performance. The specified level of performance shall be system-specific based on mission needs.

- Flexibility. Systems' HGI shall maximize the extent to which the system can accommodate changes to the end-user tasks beyond those initially specified. This includes providing multiple methods of accomplishing a task for various skill levels or user preferences.
- Tailorability. Systems' HGI shall maximize the extent to which the system can accommodate mission changes, user preferences, or experience level as well as the specific needs of the presentation device.

f. Task Efficiency. *Systems' HGI shall provide decision aids and tools, as necessary, to maximize user efficiency and performance of their task, with operator aids designed to support specific user tasks and tailored to the information needs of the targeted user* **(*Threshold*)**.

g. User-Centered Design. *A user-centered design process and user testing shall be employed for systems' HGI to ensure that the end-user's cognitive frameworks and expectations are accommodated by the system design* **(*Threshold*)**. A user-centered design process, executed early during system development through a series of user evaluations and refinements, ensures that the requirements of the end-user are satisfied and results in increased user satisfaction with the final system.

h. Standards. *Systems' HGI shall be compliant with the DoD JTA and other DoD CIO prescribed standards and architectures* **(*Threshold*)**.

i. Adaptability. *Systems' HGI shall provide for information presentation that is tailored to the specific needs of the user as defined by decision-making requirements, mission needs, etc., shall be consistent wherever it is displayed* **(*Threshold*)**.

j. Neutrality. *Systems' HGI presentation format shall not change the intended meaning of the information being presented; thus all data shall be clearly labeled to avoid misinterpretation or confusion* **(*Threshold*)**.

k. Ergonomics. *To minimize user fatigue and discomfort, systems' HGI hardware and software elements shall be ergonomically designed with respect to the user's operating environment* **(*Objective*)**.

l. Errors. *Systems' HGI shall be designed to minimize user input/mechanical/perception errors* **(*Threshold*)**.

m. On-line Help. *Systems' HGI shall provide context-sensitive on-line help at the user's request, thus eliminating/reducing the need for off-line support or documentation that may distract the user from the intended task* **(*Threshold*).**

5. Network Operations

Network Operations is the organizational and procedural structure used to monitor, manage, and control the Global Information Grid by means of the GIG functions of Network Management, Information Dissemination Management, and Information Assurance.

a. Network Management (NM) Function

(1) General. Network Management is the set of activities that establishes and maintains the GIG network switching, transmission, information services, and computing resources available to fulfill users' telecommunications and connectivity needs and demands. Key Network Management services are fault, configuration, account, performance, and planning management.

(2) GIG End-to-End Situational Awareness. Network managers must have real-time knowledge of the network. This knowledge must encompass awareness of all aspects of the network, including all network assets, their physical location, and their logical relationship within the network. *To accomplish GIG end-to-end situational awareness, systems shall have the NM capability of automatically generating and providing an integrated/correlated presentation of networks and all associated network assets* **(*Threshold*)**.

(3) Dynamic, Predictive Planning. *Systems shall have the NM capability to perform dynamic, predictive planning by gathering, storing and using knowledge about GIG assets/resources, so as to optimize their utilization* **(*Threshold*)**. Knowing equipment types and quantities available to support an operation is imperative for GIG utilization planners. Initially, a database must be defined and populated with organizations and their known GIG assets/resources. Once defined and populated, the database shall have the capability to be modified, as required, to support changing mission requirements to include activation/deactivation. The network management system shall include network design and engineering functions that account for all voice, video, and data networks that could comprise a proposed system, including commercial technology. These functions shall include automated mapping of network topology; measurement and recording of traffic flow data; trend analysis; spectrum planning and management; propagation analysis; electromagnetic resolution and electronic key management. A modeling and simulation capability shall be provided to allow a planner to assess the impact of changes to a system or network, without interrupting the operational network. *Systems shall have the NM capability to create/modify/distribute GIG network plans and orders IAW user requirements* **(*Threshold*)**.

(4) Distributed and Partitioned Network Control. *Systems shall have the NM capability to rapidly transfer control of one or more objects or groups of varying size, and reestablish control when relinquished without hindering end-to-end visibility by the senior network manager, while maintaining continuous control* **(*Threshold*)**. Only one active manager for a network object shall be permitted at any given time.

(5) Remote Object and Network Control and Configuration. Network managers must be able to monitor, configure, and control all aspects of the network and observe changes in network status. Networks comprising the GIG are evolutionary in nature and generally are comprised of both legacy and emerging systems, some with their own management systems.

Systems shall have the NM capability that leverages existing and evolving technologies and shall have the ability to perform remote network device configuration/reconfiguration of objects that have existing DoD JTA management capabilities **(*Threshold*)**.

(6) Network Status. Components of the GIG provide metrics to network managers to allow them to make decisions on managing the network. *Systems shall have the NM capability to obtain the status of networks and associated assets in near real time 99%* **(*Threshold, KPP*)** *and 99.9%* **(*Objective, KPP*)** *of the time.*

(7) Automated Fault Management. *Systems shall have the NM capability to perform automated fault management of the network, to include problem detection, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving* **(*Threshold*)**. This capability allows network managers to automatically monitor and maintain the status of the network's manageable devices, and to become aware of network problems as they occur based on the trouble tickets generated automatically by the affected object or network. Alarms will be correlated to eliminate those that are duplicate or false, initiate test, and perform diagnostics to isolate faults to a replaceable component.

b. Information Dissemination Management (IDM) Function

(1) General. Information Dissemination Management shall be utilized to maximize the flow of relevant information to the user consistent with the user's information requirements, the commander's policy and available resources. IDM shall provide awareness of, access to, and delivery of information across the GIG based on the priority of information flows set by the commander's dissemination policy, infrastructure availability, and security policies. The value of IDM increases as the access to information increases and the hierarchical relationships of information flow control are well established between the commanders within and between AORs. Additionally, the value of IDM increases as the user's specific information requirements are articulated, because the information producers can be more proactive and efficient in satisfying these requirements. IDM dependencies include robustness of the networks/communications transmission pathways, the systems on which IDM will reside, and the standardization of data, databases, and data description (metadata). Specific IDM requirements are described in sub paragraphs 2-20 below, and more comprehensively in the IDM CRD.

(2) Requirement Identification. *Systems shall have an IDM capability to assist users in efficiently defining their information requirements in a manner that captures key attributes associated with these requirements (e.g., timeliness, quantity, confidence level, etc.)* **(*Threshold*)**. This capability will facilitate rapid awareness of existing information that could satisfy the information requirement. It will also trigger the need to collect new information, minimize information overload, and optimize use of

available communications resources. This capability will provide a means of tracking and retrieving available information consistent with information and mission requirements in a manner that most effectively utilizes resources at the national, regional, and local levels.

(3) Search Driven Information. *Systems shall have an IDM capability to acquire the needed information by search queries, with successful searches yielding 85% of available, needed information based on the user query and no more than 20% (of the received information) waste* **(*Threshold, KPP*)**; *and yielding 95% of available, needed information and no more than 10% (of the received information) waste* **(*Objective, KPP*)**. *Systems shall have an IDM capability to locate and characterize available information of interest that minimizes information overload* **(*Threshold*)**.

(4) Information Advertisement. *Systems shall have an IDM capability through which an information producer's products become known to the user population* **(*Threshold*)**.

(5) Information Flow Awareness. *Systems shall have an IDM capability through which commanders become aware of the information flowing within their AOR to facilitate adjustments to meet operational mission requirements* **(*Threshold*)**. *Systems shall have an IDM capability for monitoring and tracking information flows to identify trends; for forecasting volume, content, and QoS consistent with information and mission requirements; and for predicting the results of information control policies to optimize available resources consistent with mission priorities* **(*Objective*)**.

(6) Status. *Systems shall have an IDM capability to track satisfaction of information requirements from the point of information request to delivery of requested information* **(*Threshold*)**.

(7) Controlled Access. *Systems shall have an IDM capability to regulate access to information in accordance with information assurance policies and procedures, and a commander's dissemination policy, to include the ability to constrain/control the awareness of the existence of information* **(*Threshold*)**. Specific dissemination policy will constrain browsing by those under a commander's command based on variables such as file size, type, source, resource, or location.

(8) Information Description. *Systems shall have an IDM capability to access information from the GIG using standard metadata* **(*Threshold*)**.

(9) Delivery Plan. *Systems shall have an IDM capability to build an end-to-end delivery plan based on user information requirements, mission priorities, dissemination policy, and available transport resources* **(*Threshold*)**. *Systems shall have an IDM capability to dynamically adjust delivery plans based on changes to user information requirements, mission priorities, dissemination policy, and available transport resources* **(*Objective*)**.

(10) Information Retrieval. *Systems shall have an IDM capability to retrieve information of interest once it has been located* **(*Threshold*)**.

(11) Collection Request. *Systems shall have an IDM capability to request the collection and production of information that is required by a user but is not already available* **(*Threshold*)**.

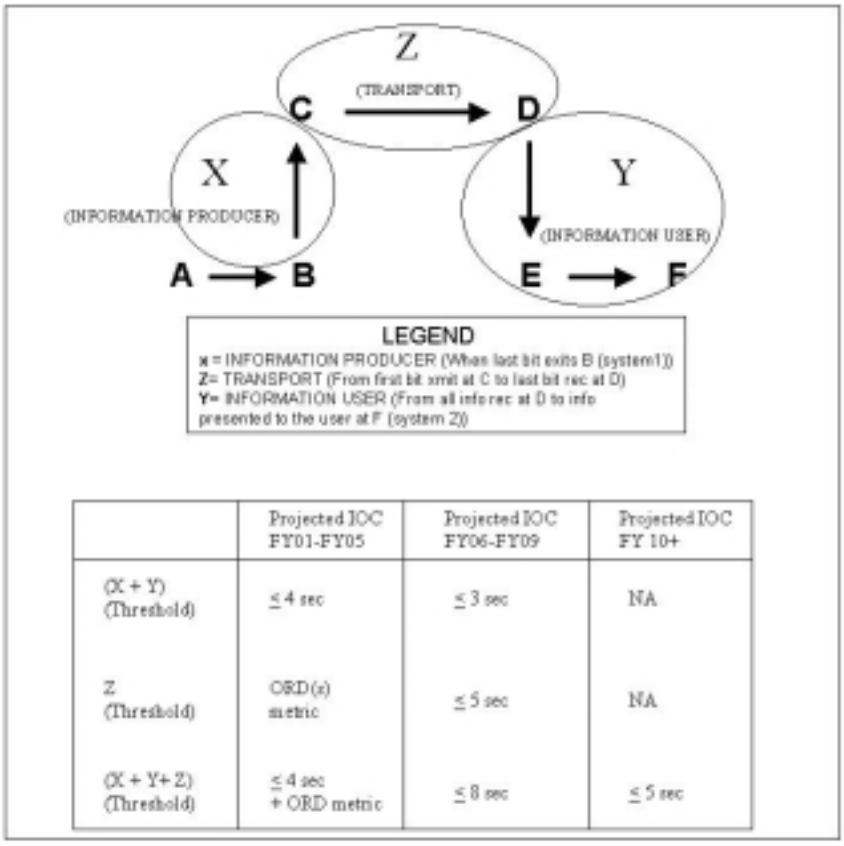
(12) Dynamic Profiling. *Systems shall have an IDM capability to activate/deactivate information requirements based on external influences such as mission, role, time, location, situation, and environment* **(*Threshold*)**.

(13) Delivery Management. *Systems shall have an IDM capability to assign attributes (e.g., priority, QoS) to information that will govern its dissemination and also a capability to convey the attributes (e.g., priority, QoS, etc.) of information to the transport system* **(*Threshold*)**. Individual information elements may have varying degrees of importance/criticality for identifiable users/groups of users. In recognition of this fact, *systems shall have an IDM capability to assign precedence to information, which will govern its dissemination throughout the GIG, and ensure that the priority for an information requirement shall be carried with all the elements of information required to satisfy that requirement, to include the capability to apply precedence to blocks of information packets for digital voice service to ensure adequate QoS* **(*Threshold*)**.

(14) Policy Management. *Systems shall have an IDM capability for commanders, and those delegated information flow authority within an organization, to dynamically adjust their information dissemination policies* **(*Threshold*).** None, some, or all components of a commander's dissemination policy may be specified. In other words, a commander may choose not to restrict access and may only assign priorities to information flows when information/communication resources are exceptionally scarce. Using IDM, a commander must be able to quickly modify a policy in response to changes in operational situations or communications resources. This enables the effective control of information to keep pace with the user's needs in the dynamic environment in which he or she is operating.

(15) Survival Information Dissemination. *Systems shall have an IDM capability that, utilizing a standard schema, IAW the commanders' dissemination policies and user profiles, will support the means for prioritization of information flows within a theater, using theater apportioned resources, and enable dissemination of survival information (limiting survival information to less than 12 kb) within the time frames of the matrix portrayed in Figure 5, 95% of the time **(Threshold, KPP)** and 0.5 seconds 95% of the time **(Objective, KPP)**.*[5]

[5] The Joint Requirements Panel (JRP) has forwarded the Survival Information Dissemination KPP (with Threshold/Objective metrics) to the Joint Requirements Board (JRB) as part of the Joint Requirements Oversight Council (JROC) approval process.



	Projected IOC FY01-FY05	Projected IOC FY06-FY09	Projected IOC FY 10+
(X + Y) (Threshold)	≤ 4 sec	≤ 3 sec	NA
Z (Threshold)	ORD (z) metric	≤ 5 sec	NA
(X + Y+ Z) (Threshold)	≤ 4 sec + ORD metric	≤ 8 sec	≤ 5 sec

Figure 5. Survival Information Dissemination Metric

(16) Correlation. *Systems shall have an IDM capability to minimize the delivery of redundant information, as well as the capability to identify complementary, parallel, or reciprocal relationships among information elements* ***(Threshold)****.* Although these IDM capabilities will not, in anyway, duplicate, substitute or replace comparable capabilities of information producer systems (e.g., Integrated Broadcast Service - IBS) or information user systems (e.g., GCCS's Common Operational Picture - COP), they are required to be interoperable with them.

(17) Notification. *Systems shall have IDM capabilities* ***(Threshold)*** *for notification of:*

- *changes in policy*
- *changes in user information requirements*
- *information becoming available or changing*

- *changes in network status that impact information flow*
- *changes in provider and user system status*
- *the delivery/receipt of information*
- *status of IDM services*
- *product availability*
- *a conflict within the delivery plan*

Systems shall have an IDM capability that gives the user the option of being notified when information related to his/her requirements becomes available or when changes occur; in the case of survival information, notification will be automatic **(*Threshold*)**.

(18) Flexibility. *Systems shall have an IDM capability that can be applied from the strategic to the tactical levels without major software modifications* **(*Threshold*)**.

(19) Scalability. *Systems shall have IDM capabilities that are scalable to meet system and operational user requirements* **(*Threshold*)**. For example, a man-portable tactical communications and computing system would include some but not all of the IDM capabilities available on a major command center C2 system.

(20) Directory Services. *Systems shall have an IDM capability that provides directory services with minimal personal intervention* **(*Threshold*)**.

c. Information Assurance (IA) Function

(1) General. Information assurance is defined as information operations that protect and defend information and/or information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and response capabilities (*Joint Publication 3-13*).

(2) Information Integrity and Availability. The GIG must be an assured system of systems with a defined and controlled security perimeter. Interconnection of GIG systems/elements to outside systems/elements should be done only in a controlled fashion using adequate assurance means. The GIG must include a protected electronic perimeter for local enclaves in accordance with *Defense in Depth Standards* (*CJCSI 6510.01C*). Therefore, *systems shall have the IA capability to define, control, and defend enclave boundaries* ***(Threshold)****. To support IA across the GIG, systems shall be robust, survivable and capable of rapid restoration* **(*Threshold*)**. *Systems shall have an IA capability that provides users with timely, reliable access to processes and data even in the event of a denial of service attack* **(*Threshold*)**. *Systems shall also have the IA capability to ensure data and process integrity throughout the system (during storage, processing, transmission and presentation) so as*

to prevent unauthorized or unintended changes, in accordance with mission specific criteria **(*Threshold*)**.

(3) Prevent Opportunity to Attack. *Systems shall be developed in accordance with Defense in Depth standards (CJCSI 6510.01C) to prevent or at least minimize the opportunity to attack; and shall have, in the event of attack, the IA capability to immediately define, detect, and respond appropriately to anomalies/attacks/disruptions from external threats, internal threats and natural causes* **(*Threshold*)**.

(4) Access Control. *Systems shall have an IA capability that provides adequate protection from user attempts to circumvent system access controls, accountability, or procedures for the purpose of performing unauthorized system operations* **(*Threshold*)**.

(5) Detection and Responses. *Systems shall incorporate a detection, reporting, and response IA infrastructure that enables rapid detection of and reaction to all sources of anomalous events and enables operational situation awareness and responses* **(*Threshold*)**.

(6) Security Domains. *Systems shall have an IA capability for operating within each security domain and across any security domains, while ensuring that all operations are conducted within the appropriate security measures* ***(Threshold*)**. *Systems shall have an IA capability to maintain 100 percent information integrity when operating at different security levels and comply with existing security requirements* **(*Threshold, KPP*).** *Systems shall comply with 100 percent of existing security requirements without waivers* **(*Objective*)**.

(7) Authentication/Confidentiality/Non-repudiation. *Systems shall meet and maintain minimum IA Defense in Depth standards, including certification and accreditation in accordance with DITSCAP process (e.g., CJCSI 6510.01C, DoDI 5200.40)* **(*Threshold/Objective, KPP*)**. *Systems shall utilize/interoperate with security management and the DoD public key infrastructure* **(*Threshold*)**. *Systems shall provide proof of origin and receipt as required* **(*Threshold*)**.

(8) Confidentiality Services. It is essential that secure operations can be conducted across security domains. *To support this, systems shall have an IA capability that ensures information is not disclosed to unauthorized entities or processes on the network and infrastructure so as to protect against passive intercept attacks, including unauthorized disclosure of information and traffic analysis* **(*Threshold*)**. *Systems shall also have an IA capability to share data among users operating at different and/or multiple security levels as appropriate (e.g., one terminal with multiple security modes, "colorless" backbone, data labeling, Allied/Coalition, unclassified through TS/SCI)* **(*Threshold*)**.

(9) Content-Based Encryption. *Systems shall have an IA capability to perform content-based encryption of information objects at the host instead of depending on the bulk encryption of the entire network in order*

to secure the information **(*Threshold*)**, *and this capability shall also be available for operations involving allied and coalition forces* **(*Objective*)**.

B. Interoperability

Interoperability is the ability of two or more systems, units, or forces to provide services to and accept services from other systems, units or forces to enable them to operate effectively together. This condition is achieved between communication-electronics systems or equipment when information or services can be exchanged directly and satisfactorily between users. The degree of interoperability that can be achieved will be primarily determined by the accomplishment of the IER fields in Appendix B. *The GIG interoperability KPP must satisfy all critical IER attributes at the threshold level* **(*Threshold*)** *and satisfy all critical IER attributes to the objective level* **(*Objective*)**.

1. Standards

Enforcement of IT and architecture standards is an essential element for achieving interoperability across the GIG.

a. Compliance. GIG systems shall be implemented in accordance with DoD CIO prescribed standards, the latest versions of the *DoD JTA*, DII COE, GIG architecture and other existing GIG and DoD directives, standards and instructions. Host nation and bilateral agreements will need to be checked for their ability to interface with the GIG. To ensure GIG interoperability is maintained, when a particular standard is lacking in the current set of IA standards, DoD CIO prescribed standards, or International standards as appropriate, the issue will be elevated along with the specific recommendation for what new standard(s) should be added, and/or what existing standard(s) should be modified or deleted.

b. Interoperability Testing and Certification. Interoperability testing and certification must be addressed as an integral part of the future requirement generation process prior to production and fielding of GIG systems regardless of ACAT level, in accordance with CJCSI 6212.01B.

c. Technology Insertion. The GIG shall apply open-system design strategies to enable the insertion of new and emerging technologies while maintaining interoperability with existing GIG systems and architectures. However, emerging technologies, for which standards do not exist, may be incorporated only if they can integrate with JTA standards and the DII COE, in a seamless and efficient manner (i.e. without compromising interoperability or GIG functionality requirements).

d. Data Standards. All GIG systems shall support standardized semantic tagging of data. Supported attributes must include, but are not limited to: classification, releasability, transport priority, and other quality of service functions. All GIG data that will be exchanged or has the potential to be exchanged, must be tagged, at a minimum, with classification and releasability information. Both the syntax and semantics of all GIG data and semantic tagging mechanisms will comply with applicable DoD standards. In

cases where standards do not exist for a class of data, the developer will be responsible for unambiguously defining the syntax and semantics.

2. Key Interoperability Requirements

The capability requirements shown in the Table 4-1 KPP Rollup below are essential for achieving interoperability, both inside the GIG and external to it.

Table 4-1. KPP Rollup

FUNCTIONAL AREA	CAPABILITY	KPP	REQUIREMENT
Interoperability	Satisfy Critical IER Attributes	✔	Systems shall satisfy all critical IER attributes at the threshold level (**Threshold, KPP**) and satisfy all critical IER attributes to the objective level (**Objective, KPP**).
Store	Data Interoperability	✔	All of a system's data that will be exchanged, or has the potential to be exchanged, shall be tagged IAW the current JTA standard for tagged data items (Extensible Markup Language [XML]), and tags will be registered in accordance with the Defense Information Systems Agency (DISA) COE Data Registry, Level 6 (**Threshold, KPP**)/ Level 8 (**Objective, KPP**).
Transport	Quality of Service	✔	Transport systems shall provide QoS capabilities that ensure that information identified as priority is delivered ahead of regular traffic 99% of the time **(Threshold, KPP)** and 99.9% of the time **(Objective, KPP).**

FUNCTIONAL AREA	CAPABILITY	KPP	REQUIREMENT
	Information Integrity	✔	Transport systems shall maintain and guarantee during transport the integrity of all information elements exchanged throughout the GIG to enable user confidence; information integrity shall be 99.99 percent (**Threshold, KPP**) and 99.999 percent (**Objective, KPP**) as specified in the Information Dissemination Management (IDM) CRD as an information delivery requirement.
	Transport Element Status	✔	All transport elements (e.g., switches, routers, etc.) shall be capable of providing status changes to network management devices by means of an automated capability in near real time 99% (**Threshold, KPP**) and 99.9% (**Objective, KPP**) of the time.
	Secure Voice Interoperability	✔	Strategic secure voice systems and tactical secure voice systems shall be interoperable, with a 99% (**Threshold, KPP**) and 99.9% (**Objective, KPP**) call throughput success rate.
Network Management	Network Status	✔	Systems shall have the NM capability to obtain status of networks and associated assets in near real time 99% (**Threshold, KPP**) and 99.9% (**Objective, KPP**) of the time.

FUNCTIONAL AREA	CAPABILITY	KPP	REQUIREMENT
IDM	Search Driven Information	✔	Systems shall have an IDM capability to acquire the needed information by search queries, with successful searches yielding 85% of available, needed information based on the user query and no more than 20% (of the received information) waste (**Threshold, KPP**); and yielding 95% of available, needed information and no more than 10% (of the received information) waste (**Objective, KPP**).
	Survival Information Dissemination	✔	Systems shall have an IDM capability that, utilizing a standard schema, IAW the commanders' dissemination policies and user profiles, will support the means for prioritization of information flows within a theater, using theater apportioned resources, and enable dissemination of survival information (limiting survival information to less than 12 kb) within the time frames of the matrix portrayed in Figure 5, 95% of the time (**Threshold, KPP**) and 0.5 seconds 95% of the time (**Objective, KPP**).[6]
Information Assurance	Security Domains	✔	Systems shall have an IA capability to maintain 100% information integrity when operating at different security levels and comply with existing security requirements **(Threshold, KPP).**

[6]The Joint Requirements Panel (JRP) has forwarded the Survival Information Dissemination KPP (with Threshold/Objective metrics) to the Joint Requirements Board (JRB) as part of the Joint Requirements Oversight Council (JROC) approval process.

.

FUNCTIONAL AREA	CAPABILITY	KPP	REQUIREMENT
	Authentication/ Confidentiality/ Non-repudiation:	✔	Systems shall meet and maintain minimum IA Defense in Depth standards, including certification and accreditation IAW DITSCAP process (e.g., *CJCSI 6510.01C*, *DoDI 5200.40*) (**Threshold/Objective, KPP**).

C. Information Exchange Requirements (IERs)

1. The GIG diagram in Figure 5 illustrates information exchange requirements for the GIG. These information exchanges become the foundation for a more complex architecture that will form the basis for detailed information exchange requirements in ORDs. Note that the diagram is intended to represent logical interactions and information flows, not physical connectivity.

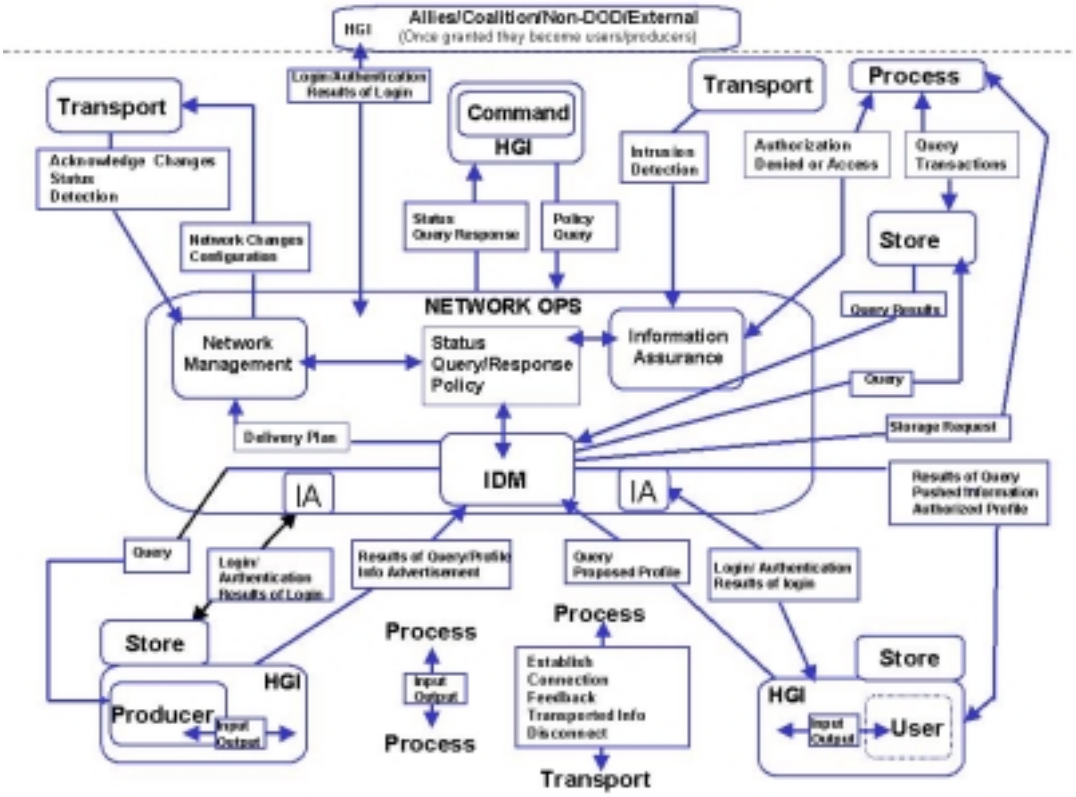


Figure 6. GIG IERs

2. The following paragraphs describe the major elements of the GIG IERs:

a. Command Node. It is organized to gather, process, analyze, display, and disseminate planning and operational data and perform other related tasks. In the objective GIG operational context, the primary command activities include:

- Conducting integrated knowledge and information management activities
- Producing integrated dissemination policies and profile guidance
- Monitoring GIG status and information flows

b. Information User. A user is any node that participates in information processes primarily as a consumer of information. A user:

- Proposes information profiles
- Performs information searches
- Receives profiled information
- Monitors status of information requests
- Can store or dispose of information

c. Information Producer. A producer is any node that participates in information processes primarily as an information producer. A producer:

- Receives and responds to information profiles
- Generates information products and standard metadata descriptions of those products
- Executes information transfers in response to on-demand requests or standing profiles
- Monitors GIG services to track the status of relevant activities

d. Allies/Coalition/and other External Systems. The external node is those external users/producers who require access to the GIG. Once access is granted, they become users/producers as required. The Network Ops Node receives the access IER so that IA, NM, and IDM can coordinate the security access, physical connection and dissemination considerations that must be made. Network Ops is receiving its external policy procedures from the command node. This node includes NSC, DOS, DOJ, FEMA, POV etc.

e. Create/Acquire and Dispose. A discussion of information exchange would be incomplete without the beginning and end of the information cycle. The Create node will be half inside and half outside of the GIG. The Dispose node appears outside of the GIG boundary because once information is disposed of, it is no longer a part of the GIG.

f. The remainder of the nodes are the functional/logical entities of the GIG described in Chapters I and IV. It should be noted that these functional entities also act as senders and/or receivers of information and will exchange information with other like nodes. For example NM to NM will exchange status information, Transport to Transport will handshake, and Store to Store will perform remote retrieval.

Note: The terms "Information User" and "Information Producer" and “Command” depend on the functions being performed by the node. Producers can also be users and vice versa.

3. Survival Information Timeliness Requirement. ORD writers will not be required to change internal IERs when:

- Sending/receiving nodes are self-contained within a system.
- External IER timeliness requirements have been verified as being interoperable (timeliness attributes for an IER between two different systems match).

ORD writers will be required to use the Survival Information Dissemination KPP timeliness attribute for external survival IERs when multiple systems are involved (provides a baseline for interoperability of survival information timeliness attributes).

4. Applicability to ORDs/CRDs. The information exchange requirements depicted in Figure 6 represent the high-level exchange requirements that can apply to any information system. Although ORDs/CRDs are written for other than information technology systems, any IER found in a non-IT CRD/ORD will always contain a sending node and receiving node which corresponds to the user and producer node in the GIG IER diagram. Although more specific in nature, the Event and Information Characterization columns will always contain one of the basic elements of user/producer exchange such as query, status, results of query, pushed profile information, and information advertisements. Not all nodes and IERS will apply to every ORD/CRD. In those cases where the IDM, IA or NM node are not applicable, the ORD/CRD writer can make a logical extension directly from the user/producer to store, process, or transport. Optional fields for a CRD that should be considered for ORDs are: timeliness, data recognition, frequency and data relevance.

5. Examples of Applicability.

Table. 4-2

Advanced Amphibious Assault Vehicle

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
TA1.1	Combat ID	PLI,SA info for surface to surface CID	AAAV(C) AAAV(P)	U.S. Armored Systems (Shooters)	Y	Pushed information

Integrated Collaborative Collection Management

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
SN 2.5	Smart Push	Send finished imagery/products to users based on pre-designated criteria.	Exploit/ Production centers	All authorized users including allies and coalition partners	Y	Pushed information * This IER should trigger the ORD writer to think about how the coalition requests and is granted access in their system because the GIG IERs include an external GIG access IER

Joint Tactical Radio System

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
OP 5.1.1	System Network Information and Status	System and Network Reports	JTRS NMS	JTRS NMS	N	Status from Transport and Process to Network Management

Defense Joint Accounting System

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
SN 4.7	Populate data warehouse		DPPS-DCD	DJAS	Y	Store Request

Global Combat Support System

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
Cross-walk contained at Appendix C.	Joint Decision Support Tools	Provide graphical displays to depict units and infrastructure Provide drill down capabilities to identify…	GCSS-A GCSS-AF GCSS-MC GCSS-M BSM JTAV JPAV GTN JOPES	NCA CINC JTF Services	Y	Request for Information

SECTION D GIG CRD COMPLIANCE CHECKLIST

ORDs under a CRD must address the CRD KPPs relevant to the particular operational purpose(s)/mission(s) they support. ORDs are not expected to address a CRD KPP or other CRD capability if it does not apply to the proposed system. This checklist includes KPPs and other capability requirements found in the GIG CRD. The ORD/CRD operational concept and information exchange requirements will determine which KPPs/capabilities are applicable. Because the GIG operates as a globally interconnected, end-to-end, interoperable system of systems, all systems that comprise the GIG shall be GIG-enabled so as to allow "plug and play" interoperability among systems. A system shall be considered GIG-enabled if it has the capabilities described in this CRD for the seven GIG functions, as appropriate and necessary to fulfill the system's operational purpose(s)/mission(s).

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
GENERAL						
GIG Reference	I.B.3	Does the GIG CRD appear in the Related Documents section?				
Operational Concept	I.E.3	If the OV-1 depicts information exchange relationships, are the producer, user, and command node entities identifiable?				
		Does the operational concept acknowledge that resources including bandwidth are finite?				
		Does the operational concept include external information exchange?				
GIG Implementation Guidelines	I.F.2	Have each of the following GIG implementation guidelines been considered and applied in the ORD as appropriate?				
		GIG implementation done in accordance with the standards included in the most current version of the *DoD JTA*?				
		All new Command, Control, Communications, Computers and Intelligence (C4I) emerging systems and upgrades to be fielded as level 6 DII COE compliant with the goal of achieving level 8 compliance?				
GIG Implementation Guidelines	I.F.2					

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
		System is either standards based or employs commercial-off-the-shelf (COTS) technologies to: - Facilitate joint, allied, and coalition interoperability? - Simplify integration? - Reduce both long and short-term costs?				
		Government-off-the-shelf (GOTS) and proprietary technologies are used only if standards-based and COTS technologies are proven to be inadequate?				
		System is to be scalable and extensible with respect to its functionality?				
		System is designed to accommodate change and facilitate the integration of future systems and technologies as they evolve?				
		System is consistent with current DoD, IC, and commercial efforts regarding data and metadata standardization?				
		GIG-enabled applications designed to reside on current or proposed DII COE compliant systems, are used, except where the requirement is waived?				
		Additional manpower requirements are minimized?				
		Emphasis is placed on reducing the complexity, time, and cost of training?				
		Software design is aimed at enhancing interoperability and commonality among GIG-enabled systems?				
		System adheres to open system standards?				
		Bandwidth and throughput requirements along with implications to strategic, fixed, theater, and tactical architectures are considered?				
		The use of NIMA standard military data is specified to be used where possible to support common operational displays of geopolitical boundaries among the commands?				
		Common operational displays are compatible with NATO standards as appropriate?				
		The system will be developed, tested, and deployed in a manner that is compliant with all appropriate treaties and international agreements?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
		The system will be tested and certified for interoperability IAW Joint Interoperability Test Command (JITC) procedures?				
		System enables users to operate in a multilingual environment to overcome the inherent language barriers of multinational and coalition operations?				
		System meets all current security provisions articulated in appropriate DoD and IC policies, procedures, and instructions including DoDD 8500.aa?				
		System uses standards-based rather than system-unique security mechanisms?				
		ORD considers ongoing developments and evolving specifications in the following areas (as applicable): - Joint Operational Architecture (JOA)? - Nuclear C2 Systems Technical Performance Criteria (NTPC)? - GIG Architecture				
THREAT						
Threat to be Countered	II.A.2	If information exchange is fundamental to the ORD/CRD, does chapter 2 mention Information Operations, Computer Network Attack, Computer Network Exploitation, Electronic Warfare, and Electromagnetic Pulse?				
SHORTCOMINGS						
Shortcomings	III.B	Does the ORD describe shortcomings or absence of existing capabilities and systems to fulfill the needs of the GIG functions described in Chapter I? As applicable, are GIG shortcomings addressed such as: lack of interoperable applications; limited ability to rapidly catalog, search, and retrieve required information; limited ability to effectively and efficiently use existing RF spectrum; limited ability to move digital information seamlessly; lack of asset visibility resulting in limited ability to effectively manage a common user network; limited means to prioritize information and establish profiles; limited ability to support multilevel security operations?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
PROCESS FUNCTION						
Processing Efficiency and Effectiveness	IV.B.1b	All computing processes of system shall optimize the use of constrained computing and dissemination resources (**Threshold**)?				
Reuse Of Information Products	IV.B.1c	System's previously generated, shareable information products (i.e., processed data) shall be reused to maximize consistency and efficiency, and to minimize process redundancy (**Threshold**)?				
Processing Mode	IV.B.1d	System shall have processes to accommodate an interactive and multimedia processing environment (**Threshold**)? System's need for other processing modes, especially batch processing, shall be clearly demonstrated and justified prior to their adoption (**Threshold**)? System shall use time-critical processing when dealing with survival information, in order to meet stringent timeliness requirements (**Threshold**)?				
Value-Added Processing	IV.B.1e	System shall have processes that add value to the information and are deemed necessary as well as essential for the implementation of the target system (**Threshold**)?				
Cohesiveness	IV.B.1f	Each process of the system shall accomplish a well-defined single function so as to achieve cohesion and enhance process reusability and system maintainability (**Threshold**)?				
Modularity	IV.B.1g	System's processes shall be modular to reduce maintenance and promote reusability (**Threshold**)?				
Process Reusability	IV.B.1h	System shall have, to the maximum extent possible, processes that are designed (using off–the–shelf standard components built according to an open standard) and implemented to be reusable in multiple systems and computing environments as plug and play "commodities" or "generics" rather than custom built from scratch each time (**Threshold**)?				
Reliability	IV.B.1i	System shall have processes that are classified either as deterministic or non-deterministic, with each deterministic process producing consistent and definite results, and each non-deterministic process specifying a range with boundary limits and the expected average for each output generated (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Validation	IV.B.1j	The accuracy of outputs from the system's processes, deterministic or otherwise, shall be testable, meaning that processes shall be executable and the actual outputs generated by a process shall conform to expected outputs governed by operational requirements (**Threshold**)? In the case of the system's non-deterministic processes, it shall be possible to predict all outputs within specified limits (**Threshold**)?				
Verifiability	IV.B.1k	System shall have processes that facilitate verification, and verification activities shall be performed to discover design errors and demonstrate the conformance of the system to the specified requirements (**Threshold**)?				
Interprocess Communications	IV.B.1l	To achieve interoperability among the system's processes, all processes shall use standardized mechanisms to communicate with each other, and process interfaces shall follow established standards for interprocess communications regardless of whether they are communicating with processes residing within the same computing system or with processes residing on remote systems (**Threshold**)?				
Process Prioritization	IV.B.1m	System's processes shall be responsive to task prioritization dynamically (**Threshold**)?				
Process Adaptability	IV.B.1n	All critical processes of the system shall have the capability to monitor the available resources and dynamically adjust their processing characteristics and behavior in accordance with the resources made available for their use (**Threshold**)?				
Standards-Based Processing	IV.B.1o	All processes of the system shall demonstrate compliance with existing directives, instructions, and prescribed standards (**Threshold**)?				
Process Security	IV.B.1p	All processes of the system shall be protected and secured at appropriate levels and be visible to and cooperate with all information assurance operations (**Threshold**)?				
Non-GIG Interoperability	IV.B.1q	System's processing shall accommodate non-DoD (**Threshold**) and allied and coalition (**Objective**) operations when necessary?				
Robust & Flexible Processing	IV.B.1r	All process failures and processing exceptions of the system shall be handled through error handling and recovery mechanisms which are consistent with threat and risk levels associated with the processing task (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Analytical and Collaboration Services	IV.B.1s	System's processing shall support analytical and collaboration capabilities through services that support collaborative planning, decision-making aids, modeling and simulation, data mining, intelligent agents and virtual workspaces (**Threshold**)?				
Information Management Support	IV.B.1t	System's processing shall accommodate all Information Management (IM) tasks related to creation, acquisition, transmission, organization, storage, dissemination, presentation, protection and disposition of information, as well as other information processing tasks guided by and in compliance with the DoD CIO IM Strategic Plan (**Threshold**)?				
Interface Definition	IV.B.1u	All process interfaces of the system shall be well defined and clearly specified to include at a minimum all input specifications, output specifications, and specifications for controls required for triggering the process (**Threshold**)?				
Cross Platform Functionality	IV.B.1v	System's processes shall be independent of the computing platform regardless of the programming or scripting (**Threshold**)?				
Process Availability	IV.B.1. w	System's processing components shall ensure that the overall system availability is not compromised due to run-time process failures (**Threshold**)?				
STORE FUNCTION						
Data Interoperability	IV.B.2b	All of the system's data that will be exchanged, or has the potential to be exchanged, shall be tagged IAW the current JTA standard for tagged data items (Extensible Markup Language [XML]), and tags shall be registered in accordance with the Defense Information Systems Agency (DISA) Common Operating Environment (COE) Data Registry, Level 6 (**Threshold, KPP**)/ Level 8 (**Objective, KPP**)? System shall identify and use common standards for data and metadata representation (**Threshold**)?				
Data Integrity	IV.B.2c	System's storage process shall not alter stored data in a manner that compromises the integrity of the data without the user's knowledge and consent (**Threshold**)?				
Infrastructure Management	IV.B.2d	System shall provide visibility of storage infrastructure to efficiently manage storage capacity and provide the capability to remove/discard stored data as required (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Data Distribution	IV.B.2e	System's data shall be stored in a manner that facilitates distribution IAW processing and transport needs and supports the rapid retrieval of information by the user (**Threshold**)? Each item of stored data in the system shall have a single discrete source of reference so that future updates of that data, while being stored in other locations, will be able to refer back to the single reference source, thus ensuring that the information is being updated with the most current available version (**Threshold**)?				
Data Survivability	IV.B.2f	System's data shall be stored in a manner that assures the required access to and use of all needed data, and in a way that prevents the loss of stored data from physical threats such as fire, water damage, information operation threats, and Electromagnetic Pulse (EMP) as appropriate to the information being stored (**Threshold**)?				
Data Security	IV.B.2g	System's data being stored shall include its classification and releasability criteria within the semantic tag or associated schema (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Data Disposal	IV.B.2h	System's data that is no longer required shall be disposed of effectively and efficiently, so that the storage space that was used by the disposed data can be used for the storage of new data without the user having to do any additional actions once the decision to dispose has been made (**Threshold**)?				
Data Retention	IV.B.2i	System's data shall be retained in a manner that meets all mission and regulatory guidance and is transparent to the user (**Threshold**)?				
TRANSPORT FUNCTION						
Switching/ Routing/ Transmission	IV.B.3b	System providing switching, routing, and transmission control capabilities/mechanisms shall be fully interoperable and work seamlessly across the entire GIG in accordance with *DoD JTA* (**Threshold**)?				
Spectrum Supportability/ Electromagnetic Environmental Effects	IV.B.3c	System shall optimize use of the available electromagnetic spectrum through efficient frequency reuse and advanced modeling, compression and filtering techniques, and shall comply with DoD, National and International spectrum management policies as applicable (**Threshold**)? System shall be mutually compatible with other systems, including allied and coalition systems, in the operational environment and shall not be degraded by electromagnetic environmental effects (**Objective**). Spectrum certification and an electromagnetic environmental effects limitations/vulnerabilities report shall be obtained for 95% of systems **(Threshold)** and 99% of systems **(Objective)**?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Quality of Service	IV.B.3d	Transport system shall provide QoS capabilities that ensure that information identified as priority is delivered ahead of regular traffic 99% of the time **(Threshold, KPP)** and 99.9% of the time **(Objective, KPP)?** Required QoS factors include: • Prioritization. End users shall be able to assign priority to information targeted for transport **(Threshold)**? • Response Time. All transport capabilities shall be designed to meet or exceed customer stated response times **(Threshold)**? • Precedence. Data shall receive expedited handling during transport in accordance with the commander's policy and user assigned priority **(Threshold)**? • Reliability. Delivery of information shall be guaranteed in accordance with its assigned broadcast level **(Threshold)**? • Latency. It shall be possible to deliver information in real and/or near real time as required **(Threshold)**?				
Information Integrity	IV.B.3e	Transport system shall maintain and guarantee during transport the integrity of all information elements exchanged throughout the GIG to enable user confidence; information integrity shall be 99.99 percent (**Threshold, KPP**) and 99.999 percent (**Objective**), as specified in the Information Dissemination Management (IDM) CRD as an information delivery requirement?				
Standards	IV.B.3f	To ensure system interoperability across the GIG and to support uninterrupted service, all GIG transport capabilities shall be standards-based using *DoD JTA* and DoD CIO prescribed standards, as applicable (**Threshold**)?				
Connectivity	IV.B.3g	Transport system shall provide connectivity on demand to all fixed and deployed locations/users (**Threshold**)? Transport systems shall have the ability to maintain network connectivity on-the-move to meet Service/JTF requirements in all warfighting environments (afloat, sub-surface, airborne, in space, on the ground) (**Objective**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Capacity	IV.B.3h	With minimal exceptions, GIG transport capacity shall be viewed as an open system that is available to transport information from all domains utilizing unicast, multicast, and broadcast techniques to provide information on demand to the warfighter/decision maker (**Threshold**)? Transport system shall have the reserve capacity to accommodate surge loading and support multiple military operations as described in Defense Planning Guidance (**Objective**)?				
Technology Insertion	IV.B.3i	To effectively keep pace with advances in technology that have the potential to render existing systems obsolete shortly following acquisition, the GIG shall enable and support the seamless and efficient insertion and incorporation of emerging (future) technologies into the transport domain (**Threshold**)?				
Security	IV.B.3j	System shall provide link and transmission security based on the level of risk acceptable to the user, and the GIG security architecture shall support use of clear headers (**Threshold**)?				
Robustness	IV.B.3k	To avoid any single point of failure, the GIG shall use multiple connectivity paths (not susceptible to the same threat) and media (**Threshold**)?				
Scalability	IV.B.3l	Transport capability shall be scalable and adaptable to meet dynamic needs of users (**Threshold**)?				
Survivability	IV.B.3 m	Transport system shall be protected against all potential threats commensurate with the operating environment and the criticality of the information being transported, and shall also ensure connectivity through the total threat environment (i.e. conventional and nuclear) (**Threshold**)?				
Availability/ Reliability		Transport capabilities shall be available to provide reliable information exchange services to the warfighter/decision maker on demand and shall be responsive to the criticality of the information to be exchanged (**Threshold**)?				
Tactical Deployability	IV.B.3o	Transport system supporting tactical forces shall minimize lift requirements and be transportable using existing JTF/Service notional lift capability (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Transport Element Status	IV.B.3p	All transport elements (e.g., switches, routers, etc.) shall be capable of providing status changes to network management devices by means of an automated capability in near real time 99% (**Threshold, KPP**) and 99.9% (**Objective KPP**) of the time?				
Secure Voice Interoperability	IV.B.3q	Strategic secure voice systems and tactical secure voice systems shall be interoperable, with a 99% (**Threshold, KPP**) and 99.9% (**Objective, KPP**) call throughput success rate?				
Secure Voice with Allied and Coalition Forces	IV.B.3r	Secure voice cryptography shall be provided to or developed with allied forces that enables interoperability (**Threshold**)? Secure voice systems shall be interoperable with coalition forces (**Objective**)? A secure voice system shall be able to be provided to coalition forces that is interoperable with the U.S. version using coalition releasable technology (**Threshold**)?				
HUMAN-GIG INTERACTION (HGI) FUNCTION						
Output/Input	IV.B.4b	System's HGI shall present to and accept information from humans using a combination of visual, aural, tactile, and/or other sensory methods (**Threshold**)?				
Feedback	IV.B.4c	System's HGI shall provide unobtrusive confirmations of user input and actions, to include implicit visual, aural and/or tactile feedback in response to user actions, as well as, explicit notifications that entered data was properly entered and accepted by the system, and/or errors were detected (**Threshold**)?				
Specialized Environments	IV.B.4d	System's HGI shall functionally accommodate use in a nuclear, biological, and chemical (NBC) or other specialized operating environment as designated by mission needs (**Threshold**)?				
Usability	IV.B.4e	System's HGI shall be useable by all end user skill levels in the aspects of learnability, flexibility, and tailorability, which shall be verified by iterative user testing (**Threshold**)?				
Task Efficiency	IV.B.4f	System's HGI shall provide decision aids and tools as necessary to maximize users' efficiency and performance of their task, with operator aids designed to support specific user tasks and tailored to the information needs of the targeted user (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Design	IV.B.4g	A user-centered design process and user testing shall be employed for the system's HGI to ensure that the end-user's cognitive framework and expectations are accommodated by the system design (**Threshold**)?				
Standards	IV.B.4h	System's HGI shall be compliant with the DoD JTA and other DoD CIO prescribed standards and architectures (**Threshold**)?				
Adaptability	IV.B.4i	Systems' HGI shall provide for information presentation that is tailored to the specific needs of the user as defined by decision-making requirements, mission needs, etc., shall be consistent wherever it is displayed (Threshold)?				
Neutrality	IV.B.4j	System's HGI presentation format shall not change the intended meaning of the information being presented; thus all data shall be clearly labeled to avoid misinterpretation or confusion (**Threshold**)?				
Ergonomics	IV.B.4k	To minimize user fatigue and discomfort, the system's HGI hardware and software elements shall be ergonomically designed with respect to the user's operating environment (**Objective**)?				
Errors	IV.B.4l	System's HGI shall be designed to minimize user input/mechanical/perception errors (**Threshold**)?				
On-line help	IV.B.4 m	System's HGI shall provide context-sensitive on-line help at the user's request, thus eliminating/reducing the need for off-line support or documentation that may distract the user from the intended task (**Threshold**)?				
NETWORK MANAGEMENT (NM) FUNCTION						
Situational Gig End to End Awareness	IV.B.5a	To accomplish GIG end-to-end situational awareness, system shall have the NM capability of automatically generating and providing an integrated/correlated presentation of network and all associated network assets (**Threshold**)?				
Dynamic, Predictive Planning	IV.B.5a	System shall have the NM capability to perform dynamic, predictive planning by gathering, storing and using knowledge about GIG assets/resources, so as to optimize their utilization (**Threshold**)? System shall have the NM capability to create/modify/distribute network plans and orders IAW user requirements (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Distributed and Partitioned Network Control	IV.B.5a	System shall have the NM capability to rapidly transfer control of one or more objects or groups of varying size, and reestablish control when relinquished without hindering end-to-end visibility by the senior network manager, while maintaining continuous control (**Threshold**)?				
Remote Object and Network, Control and Configuration	IV.B.5a	System shall have the NM capability to leverage existing and evolving technologies and shall have the ability to perform remote network device configuration/reconfiguration of objects that have existing DoD JTA management capabilities (**Threshold**)?				
Network Status	IV.B.5a	System shall have the NM capability to obtain the status of networks and associated assets in near real time 99% (**Threshold, KPP**) and 99.9% (**Objective, KPP**) of the time.				
Automated Fault Management	IV.B.5a	Systems shall have the NM capability to perform automated fault management of the network, to include problem detection, fault correction, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving (**Threshold**)?				
INFORMATION DISSEMINATION MANAGEMENT (IDM) FUNCTION						
Requirement Identification	IV.B.5b	System shall have an IDM capability to assist users in efficiently identifying their information requirements in a manner that captures key attributes associated with these requirements (e.g., timeliness, quantity, confidence level, etc.) (**Threshold**)?				
Search Driven Information	IV.B.5b	Systems shall have an IDM capability to acquire the needed information by search queries, with successful searches yielding 85% of available, needed information based on the user query and no more than 20% of the received information that is not needed (waste or failed searches) (**Threshold, KPP**); and yielding 95% of available, needed information and no more than 10% of the received information that is not needed (waste or failed searches) (**Objective, KPP**)? System shall have an IDM capability to locate and characterize available information of interest that minimizes information overload (**Threshold**)?				
Information Advertisement	IV.B.5b	System shall have an IDM capability through which an information producer's products become known to the user population (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Information Flow Awareness	IV.B.5b	System shall have an IDM capability through which commanders become aware of the information flowing within their AOR to facilitate adjustments to meet operational mission requirements (**Threshold)**? System shall have an IDM capability for monitoring and tracking information flows to identify trends; for forecasting volume, content, and quality of service consistent with information and mission requirements; and for predicting the results of information control policies to optimize available resources consistent with mission priorities (**Objective**)?				
Status	IV.B.5b	System shall have an IDM capability to track and report the status of the satisfaction of information requirements from the point of information request to delivery of requested information (**Threshold**)?				
Controlled Access	IV.B.5b	System shall have an IDM capability to regulate access to information in accordance with information assurance policies and procedures, and a commander's dissemination policy, to include the ability to constrain/control the awareness of the existence of information (**Threshold**)?				
Information Description	IV.B.5b	System shall have an IDM capability to access information from the GIG using standard metadata (**Threshold**)?				
Delivery Plan	IV.B.5b	System shall have an IDM capability to build an end-to-end delivery plan based on user information requirements, mission priorities, dissemination policy, and available transport resources (**Threshold**)? System shall have an IDM capability to dynamically adjust delivery plans based on changes to user information requirements, mission priorities, dissemination policy, and available transport resources (**Objective**)?				
Information Retrieval	IV.B.5b	System shall have an IDM capability to retrieve information of interest that has been located (**Threshold**).				
Collection Request	IV.B.5b	Systems shall have an IDM capability to request the collection and production of information that is required by a user but that is not already available (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Dynamic Profiling	IV.B.5b	System shall have an IDM capability to activate/deactivate information requirements based on external influences such as mission, role, time, location, situation, and environment (**Threshold**)?				
Delivery Management	IV.B.5b	System shall have an IDM capability to assign attributes (e.g., priority, QoS) to information that will govern its dissemination and also provide a means to convey the attributes (e.g., priority, QoS, etc.) of information to the transport system (**Threshold**)? System shall have an IDM capability to assign precedence for information, which will govern its dissemination throughout the GIG, and shall ensure that the priority for an information requirement shall be carried with all the elements of information required to satisfy that information requirement, to include the ability to apply precedence to blocks of information packets for digital voice service to ensure QoS (**Threshold**)?				
Policy Management	IV.B.5b	System shall have an IDM capability for commanders, and those delegated information flow authority within an organization, to dynamically adjust their information dissemination policies (**Threshold**)?				
Survival Information Dissemination	IV.B.5b	System shall have an IDM capability that supports and enables dissemination of survival information within n seconds (TBD) 95% of the time **(Threshold, KPP)** and n seconds (TBD) 95% of the time **(Objective, KPP)**? Note: Awaiting results of the JROC-directed Tiger Team.				
Correlation	IV.B.5b	System shall have an IDM capability to minimize the delivery of redundant information as well as the capability to identify complimentary, parallel or reciprocal relationships among information elements **(Threshold)**?				
Flexibility	IV.B.5b	System shall have IDM capabilities that can be applied from the strategic to the tactical levels without major software modifications **(Threshold)?**				
Scalability	IV.B.5b	System shall have IDM capabilities that are scalable to meet system and operational user requirements **(Threshold)**?				
Directory Services	IV.B.5b	System shall have an IDM capability that provides directory services with minimal personal intervention **(Threshold)**?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Notification	IV.B.5b	System shall have IDM capabilities (**Threshold**) for notification of: • changes in policy? • changes in user information requirements? • information becoming available or changing? • changes in network status? • changes in provider and user system status? • the delivery/receipt of information? • status of IDM services? • product availability? • a conflict within the delivery plan? System shall have an IDM capability that gives the user the option of being notified when information related to his/her requirements becomes available or when changes occur; in the case of survival information, notification will be automatic (**Threshold**)?				
INFORMATION ASSURANCE (IA) FUNCTION						
Prevent Opportunity to Attack	IV.B.5c	System shall be developed in accordance with IA Defense in Depth standards (CJCSI 6510.01C) to prevent or at least minimize the opportunity for attack; and shall have, in the event of an attack, the IA capability to immediately define, detect and respond appropriately to anomalies/attacks/disruptions from external threats, internal threats and natural causes **(Threshold)**?				
Information Integrity and Availability	IV.B.5c	System shall be robust, survivable and capable of rapid restoration, to support IA across the GIG **(Threshold)**? System shall have an IA capability to define, control, and defend enclave boundaries (**Threshold**)? System shall have an IA capability to provide timely, reliable access to processes and data even in the event of a denial of service attack (**Threshold**)? System shall have an IA capability to ensure data and process integrity throughout the system (during storage, processing, transmission and presentation) to prevent unauthorized or unintended changes, in accordance with mission specific criteria **(Threshold)**?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Access Control	IV.B.5c	System shall have an IA capability that provides adequate protection from user attempts to circumvent system access controls, accountability or procedures for the purpose of performing unauthorized system operations **(Threshold)**?				
Detection and Responses	IV.B.5c	System shall incorporate a detection, reporting and response IA infrastructure that enables rapid detection of and reaction to anomalous events, and enables operational situation awareness and responses **(Threshold)**?				
Security Domains	IV.B.5c	System shall have an IA capability to maintain 100% information integrity when operating at different security levels and comply with existing security requirements **(Threshold, KPP)?** System shall comply with 100% of existing security requirements without waivers **(Objective)?** System shall have an IA capability for operating within each security domain and across any security domains while ensuring that all operations are conducted within appropriate security measures (**Threshold**)?				
Authentication/ Confidentiality/Non-repudiation	IV.B.5c	System shall meet and maintain minimum IA Defense in Depth standards, including certification and accreditation IAW DITSCAP process (e.g., *CJCSI 6510.01C*, *DoDI 5200.40*) (**Threshold/Objective, KPP**)? System shall utilize/interoperate with the security management infrastructure (e.g., key management and DoD public key infrastructure) (**Threshold**)? System shall provide proof of origin and receipt as required (**Threshold**)?				
Confidentiality Services	IV.B.5c	System shall have an IA capability that ensures information is not disclosed to unauthorized entities or processes on the network and infrastructure so as to protect against passive intercept attacks, including against unauthorized disclosure of information and traffic analysis **(Threshold)**? System shall have an IA capability to share data among users operating at different and /or multiple security levels as appropriate (**Threshold**)?				

ORD/CRD AUTHORS' GIG CRD COMPLIANCE CHECKLIST						
CRD Section Heading	**CRD Para #**	**REQUIREMENT**	**ORD Page #**	**ORD Para #**	**ORD Line #**	**YES, NO, N/A**
Content-Based Encryption	IV.B.5c	System shall have an IA capability to perform content-based encryption of information objects at the host instead of depending on the bulk encryption of the entire network in order to secure the information (**Threshold**), and this capability shall also be available for operations involving allied and coalition forces (**Objective**)?				

1

Appendix A

Part I References

1. 2000 JWSTP (Joint Warfighting Science and Technology Plan).Proposed
2. Federal Standard 1037C, Telecommunications Glossary of Telecommunications Terms, National Telecommunications Information Administration, 1997 (http://glossary.its.gov/fs-1037)
3. DoD CIO GIG Information Assurance Implementation Guidance 10 Apr 00
4. DoD CIO Guidance and Policy Memo No. 6-8510
5. DoD CIO Guidance and Policy Memo No. 10-8460
6. DoD Directive 4630.5, 12 November 1992, “Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C3I) Systems”
7. DoD Instruction 4630.8, 18 November 1992, “Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C3I) Systems”
8. DoD Directive 5000.1, 23 October 2000, “Defense Acquisition”
9. DoD Regulation 5000.2-R (Interim), 04 January 2001, “Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs”
10. DoD Electronic Desk Reference Set, “Defense Acquisition Deskbook,” December 1999
11. CJCSI 3170.01A, Requirements Generation System, dated 11 Aug 99
12. CJCSI 3222.01 CJCS Requirements for High Altitude Electromagnetic Pulse Protection of C3 Nodes and Systems
13. CJCSI 6210.02, Attack Information and Operational Architecture of the Integrated Tactical Warning and Attack Assessment System
14. CJCSI 6211.02A, Defense Information System Network (DISN) and Connected Systems, May 1996
15. CJCSI 6811.01A, Nuclear Command and Control Systems Technical Performance Criteria (NTPC), 9 June 2000
16. Concept for Future Joint Operations: Expanding JV 2010.
17. DARPA, AITS JPO Sources
18. DII Master Plan, V 8.0, “Implementing the Global Information Grid”, 24 May 1999
19. DoDD 8000.1D, Defense Information Management Program, dated 27 Oct 92
20. DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 7 October 1999
21. DoN IT Standards Guidance, V 98-1.1
22. DoDD 5200.28, Security Requirements for Automated Information Systems
23. Joint Pub 6-0, Doctrine for C4 Systems to Joint Operations, 30 May 1995

24. Information Dissemination Management (IDM) CRD, USJFCOM, 22 January 2001
25. Joint Pub 1-02
26. Joint Publications 3-13 Information Operations
27. Joint Vision 2010
28. Joint Vision 2020
29. NCSC-TG-004, Glossary of Computer Security Terms, 21 October 1988
30. NCSC-TG-016, Guidelines for Writing Trusted Facility Manuals
31. NCSC-TG-029, Introduction to Certification and Accreditation
32. Newton's Telecom Dictionary (15th Edition)
33. NTISSI No. 4009, National Security Telecommunications Information Systems Security Instruction, National Information Systems Security Glossary, 5 June 1992
34. McGraw-Hill Illustrated TELECOM Dictionary (2nd Edition)
35. CJCS Instruction 6212.01B, 8 May 2000, "Interoperability and Supportability of National Security Systems and Information Technology Systems"
36. C4ISR Architecture Framework, Version 2.0, 18 December 1997
37. Information Assurance Through Defense in Depth, Joint Chiefs of Staff, February 2000
38. DoD Joint Technical Architecture, Version 3.0, 15 November 1999
39. DoD Instruction Technology Security Certification and Accreditation Process (DITSCAP)
40. Telecom Glossary 2000 (http://glossary.its.bldrdoc.gov/projects/telecomglossary2000)

Part II Definitions.

The following is a list of terms that will help in the development of operational requirements. The official telecommunications glossary is *Federal Standard 1037C of 1996* which can be found at: http://glossary.its.bldrdoc.gov/fs-1037/ and is maintained by the U.S. Department of Commerce, National Telecommunications and Information Administration, Institute for Telecommunications Sciences. Under an approved T1 standards project (LB 837), a previously developed 5800-entry, search-engine equipped, hypertext telecommunications glossary, currently on the Web at http://glossary.its.bldrdoc.gov/projects/telecomglossary2000 is being updated and expanded for proposal as an American National Standard (ANS).

Access. The ability and means necessary to store data in, to retrieve data from, to communicate with, or to make use of any resource of a system (*Fed Std 1037*).

Access Control. A service feature or technique used to permit or deny use of the GIG components of a communication system (*Fed Std 1037*).

Advertise. Producer's activity of identifying and publishing information so that users become aware of products (*IDM CRD*).

Application. Software that performs a specific task or function, such as word processing, creation of spreadsheets, generation of graphics, facilitating electronic mail (*T1-2000*).

Architecture. (1) The design principles, physical configuration, functional organization, operational procedures, and data formats used as the bases for the design, construction, modification, and operation of a communications network. (2) The structure of an existing communications network, including the physical configuration, facilities, operational structure, operational procedures, and the data formats in use (*MIL STD 188*).

Assurance. Grounds for confidence that an information-technology (IT) product or system meets its security objectives (*T1-2000*).

Authorization. (1) The rights granted to a user to access, read, modify, insert, or delete certain data, or to execute certain programs (*Fed Std 1037C*). (2) Access rights granted to a user, program, or process (*NSTISSI 4009*).

Availability. Ensures resources and data are in place, at the time and in the form needed by the user (*IA6-8510*).

Awareness. An aggregation of functional entities providing information about the available sources of data and their current contents in order to provide efficient and effective access to that data (*IDM CRD*).

Business Functions. DoD functions that are performed but, are not war fighting or Intelligence Community specific.

Catalog. A searchable set of metadata or indices of information products, with links to sources and locations (and possibly related metadata) (*IDM CRD*).

Cataloging. The process of establishing and/or maintaining a catalog (*IDM CRD*).

Collect. Acquiring or gathering and initial filtering of information based on a planned need, determining time sensitivity and putting the information into a form suitable for transporting.

Commander. (1) The person entitled to issue IDM policy and to exercise control over information and information system resources to effectively perform a mission (*IDM CRD*). (2) A person responsible for the welfare and performance of a command in accomplishing its mission. (3) Any authority whose organization defines, operates, and controls resources that participate in information processes. Commanders establish information policies, allocate resources that control those processes, and monitor their execution. (4) Any one or more personnel who are assigned and/or delegated authority, responsibility, and resources to perform a specific DoD activity.

Commander's Dissemination Policy (CDP). Expression of a set of information awareness, access, and delivery (infrastructure allocation) requirements and constraints that controls the flow of information within the commander's domain operation of IDM components and elements; issued by a commander or designee (*IDM CRD*).

Command Node. Any node from which a command or other organizational authority performs command activities. In the objective IDM operational context, primary command activities include (a) conducting integrated knowledge and information management activities, (b) producing integrated dissemination policies and profiles, and (c) IDM status monitoring (*IDM CRD*).

Common Operating Environment (COE). The collection of standards, specifications, and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces (APIs), runtime environment definitions, reference implementations, and methodology that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product (*DII COE I&RTS*).

Compilation. Information resulting from assembly of selected information elements or information requirements from multiple sources (*IDM CRD*).

Configuration Management. It identifies, controls, accounts for, and audits all changes made to a site or information system during its design, development, and operational life cycle (*DoD CIO Guidance IA6-8510 IA*).

Confidentiality. Of classified or sensitive data, the degree to which the data have not been compromised; i.e., have not been made available or disclosed to unauthorized individuals, processes, or other entities (*T1-2000*).

Correlation. To put or bring into casual, complementary, parallel, or reciprocal relation. (IDM CRD) In intelligence usage, the process that associates and combines data on a single entity or subject from independent observation, in order to improve the reliability or creditability of the information (*JP1-02*).

Control. Control of a network resource implies an ability to monitor the resource, but also includes the ability to manipulate the functioning of that resource or to allocate it to a specific use (*DoD CIO Guidance 10-8460 NM*).

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned. (*JP1*)

Data Format. The semantics and syntax of the actual data structure. While there are many data formats in use, they may be categorized into a few basic sub-types based on the type of information they contain (e.g., textual, imagery, 3-D graphics).

Data Integrity. The condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. (*T1-2000*)

Data Standardization. The process of reviewing and documenting the names, meaning, and characteristics of data elements so that all users of the data have a common, shared understanding of it.

Defense-In-Depth. The security approach whereby layers of IA solutions are used to establish an adequate IA posture. Implementation of this strategy also recognizes that, due to the highly interactive nature of the various systems and networks, IA solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured. (*DoD CIO Guidance 6-8510 IA*)

Defense Information Infrastructure (DII). The DII is the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of DoD users across the range of military operations. It encompasses: (1) sustaining base, tactical, DoD-wide information systems, and Command, Control, Communications, Computers, and Intelligence (C4I) interfaces to weapons systems; (2) the physical facilities used to collect, distribute, store, process and display voice, data, and video; (3) the applications and data engineering tools, methods, and processes to build and maintain the software that allow Command and Control (C2), Intelligence, Surveillance, Reconnaissance and Mission Support users to access and manipulate, organize and digest proliferating quantities of information; (4) the standards and

protocols that facilitate interconnection and interoperation among networks; and (5) the people and assets which provide the integrating design, management, and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use.

Defense Information Infrastructure (DII) Common Operating Environment (COE). An application-independent basis for DoD information system architectures. The DII-COE consists of reusable software components, a plugable framework and software infrastructure, and a set of guidelines and standards for developing, integrating, and packaging mission applications.

Delivery. The process by which information is transferred into a mission application destination.

Directory Services. (1) The function of providing a client with access to one or more of the sub-directories within an IDM directory and includes resolution of the network addresses used to access applications, users, and commanders. (2) Directory services provide a mechanism for accessing, distributing, and maintaining an IDM directory.

Disposition. The process of deciding how to arrange or manage information by archiving, sending, or disposing of the information.

Distribution. The process of delivering information to the User.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security. (*DoD CIO Guidance IA6-8510*)

Electromagnetic Environmental Effects (E3). The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility/electromagnetic interference; electromagnetic vulnerability, electromagnetic pulse; electromagnetic protection; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects, of lightning and p-static.

Enclave. An environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN), or be based on physical location and proximity. The enclave encompasses both the network layer and the host and applications layer.

End-to-end. The inclusion of all requisite GIG components to deliver a defined capability. For the GIG, this implies all components from the user access and display

devices and sensors to the various levels of networking and processing, all associated applications, and all related transport and management services. For the DISN services, end-to-end encompasses service user to service user (e.g., PC-to-PC, phone-to-phone) (*DoD CIO Guidance 10-8460 NM*).

Environment. Aggregate of procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.

External Interface. An external interface is the boundary or common point where information is exchanged between entities within the GIG and those outside the GIG such as allies, coalition partners, educational institutions, governmental agencies, and other non-DoD establishments.

File. (1) The largest unit of storage structure that consists of a named collection of all occurrences in a database of records of a particular record type. (2) A set of related records treated as a unit; for example, in stock control, a file could consist of a set of invoices. (*T1 2000*)

Format. (1) The arrangement of bits or characters within a group, such as a word, message, or language. (2) The shape, size, and general makeup of a document. (*MIL STD 188*)

GIG-Enabled. Any system that exchanges and/or disseminates information in the manner described in the GIG definition, and is in compliance with the capability requirements stated in the GIG CRD, as appropriate and necessary to fulfill the system's operational purpose(s)/mission(s).

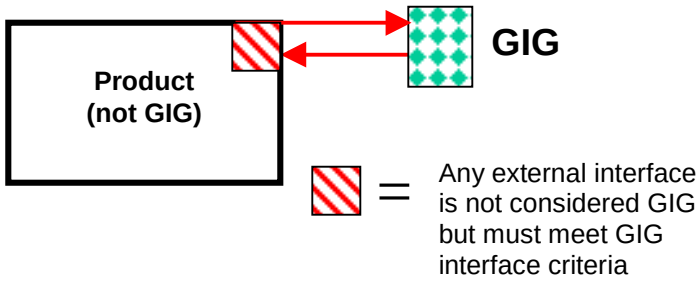
Global Information Grid. A DoD CIO memorandum dated 22 September 1999, and revised on 12 January 2001 by agreement by the DoD CIO, USD (AT&L) and Joint Staff/J6 defines the GIG as follows:

a. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related IC missions and functions (strategic, operational, tactical and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

b. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services (see paragraph c below with respect to embedded information technology).
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data or information for use by other equipment, software, and services.

c. The embedded information technology within a product is not considered part of the GIG; however, if it provides the functionality described in paragraph b above, it must meet GIG interface criteria. This is illustrated figure below:



Human-GIG Interaction (HGI). Hardware and software-enabled mechanisms and/or displays used for access and presentation of information to end users.

IDM Policy. A command statement that specifies subordinates users' awareness of and access to information, as well as precedence and priority of how that awareness and access must be achieved. IDM policies are expressed through, managed by, executed, monitored, and enforced through IDM services and tools. (*IDM CRD*)

IDM Profile. A user statement that delineates what information a specific user requires on an ongoing basis to execute all aspects of his assigned missions. It uses the IDM metadata schema to define its partitioning of the information. *(IDM CRD*)

Information. (1) The meaning that a human assigns to data by means of the known conventions used in their representation. [*JP 1-02*] (*MIL STD 188*) (2) In intelligence usage, unprocessed data of every description, which may be used in the production of intelligence. [*JP1*].

Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication,

confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities (*Joint Publication 3-13 Information Operations*).

Information Delivery. (1) An aggregation of functional entities that work together to plan and manage the transfer of data to and from application entities. The functions that are used to perform information delivery are resource monitoring, policy services, profile management, and delivery planning. (2) A process by which information providers and information users apply available information infrastructure to enable the dissemination of information, in accordance with validated profiles, consistent with commanders' policies for information transfer. The process includes translation of queries and data formats (mediation), if required, to accommodate inconsistencies between source and user systems, and subordinate delivery processes at provider locations, at intermediate waypoints within the infrastructure, and at user sites. (*IDM CRD*)

Information Dissemination Management (IDM). A set of integrated applications, processes and services that provide the capability for producers and users to locate, retrieve, and send/receive information by the most effective and efficient means in a manner consistent with a commander's policy. The fundamental IDM services, as identified in the IDM CRD, are information awareness, information access, information delivery and IDM support. Through the four services, IDM provides awareness of, access to, and delivery of information across the GIG based on the priority of information flows set by the commander's dissemination policy, infrastructure availability, and security policies (joint and combined). The value of IDM increases as the access to information increases and the hierarchical relationships of information flow control are well established between the commanders within and between AORs. Additionally, the value of IDM increases as the user's specific information requirements are articulated, because the information producers can be more proactive and efficient in satisfying these requirements. IDM dependencies include robustness of the networks/communications transmission pathways, the systems on which IDM will reside, and the standardization of data, databases, and data description (metadata).

Information Exchange Requirements. Information Exchange Requirements (IERs) express the relationship across the three basic entities of an architecture (activities, elements, and information flow) with focus on the specific aspects of the information flow. IERs identify *who* exchanges *what* information with *whom*, *why* the information is necessary, and in *what manner the exchange occurs*. (*CJCSI 3170.01*)

Information Flow. (1) Any logical transportation of any form of information across a system or network. It may originate in one or more applications, be carried through any one or more network components, and end in any one or more user applications. (2) The smallest metric of traffic that is visible from the standpoint of a network's traffic routing and management capabilities. The actual implementation of an information flow is therefore highly dependent on the network type of the networks it travels across. For example, if the network uses an IP router type of network architecture, a source and destination IP address pair would define an information flow. If the network is based on an ATM network architecture, a virtual channel identifier defines information flow. The

essential characteristic of the information flow in either case is that it represents the traffic aggregation that the network will base its resource allocation and traffic routing mechanisms on. All traffic within an information flow should therefore have similar network quality of service (QoS) requirements.

Information Infrastructure. The generic shareable resources (e.g., network elements, hosts, and information repositories) that are used to implement distributed information systems. More specifically, information infrastructure consists of those elements that may simultaneously provide multiple users with the services used to manipulate, store, and transfer data. All infrastructure falls into one of three sub-types: network, site, and information domain.

Information Management. The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructure.

Information Management Life Cycle. The total phases through which information is managed from creation through disposition.

Information Operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Processes. Any activities that collect, generate, synthesize, process, exploit, store, transport, or deliver information as part of a mission operational task.

Information Producer. A person, group, or organization that creates, updates, distributes, and retires information based on their authorized/assigned missions and functions. (*DoD CIO Guidance 6-8510 IA*)

Information Product. Data organized in a variety of forms and contexts to convey intended information in relation to other data or information to contribute knowledge needed by users; it may be in the form of a data item, object, picture, document, file, database, spreadsheet, stream or other form capable of being coherently assimilated by human or machine through visual, electronic, or audible interpretation. An information product can be a file (measured by size) or a stream (measured by duration).

Information Provider. A collector or producer of information serving information users (synonymous with a "source").

Information Superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information Superiority is achieved in a noncombat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives. (*JV 2020*)

Information System. Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment (hardware, firmware, and software) that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data.

Information Technology (IT). The hardware, firmware, and software used in an information system to perform information processing, transport, presentation, storage and retrieval functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment and also includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. (*DoD CIO Guidance*)

Information User. A person, unit, or machine using information.

Infrastructure Provider(s). Functional organization(s) responsible for the wide-area, deployed, tactical, and sustaining base telecommunications and other information services among sources, commanders, and users (e.g., DISA, BNCC).

Integrate. To coherently unite elements of disparate entities to form a single new entity.

Integrity. A combined data and information system characteristic of logical correctness and reliability of the operating system, logical completeness of the hardware and software implementing the protection mechanisms, consistent data structures, and stored data.

Interface. A boundary or point common to two or more command and control systems or subsystems, communications systems or equipment, or other entities across which necessary information flow takes place. A joint interface implies that the boundary is shared by two or more Services/Agencies.

Interoperability. (1) Ability of information systems to communicate with each other and exchange information. (2) Conditions, achieved in varying levels, when information systems and/or their components can exchange information directly and satisfactorily among them. (3) The ability to operate software and exchange information in a heterogeneous network (i.e., one large network made up of several different local area networks). (4) Systems or programs capable of exchanging information and operating together effectively.

Knowledge. (1) Having cognizance. (2) The fact or condition of knowing something with familiarity gained through experience or association of available information. (3) The fact or condition of having information or being aware of something.

Latency. The length of the time interval between an event or stimulus and a response. In the context of IT, latency refers to the amount of time it takes from the initiation of a control to the response of a control; or from an information query to the return of information.

Metadata. Data that defines other data, an information product, such as classification, format, size, keywords, etc.

Mission Application. Any information system employed by users to produce, analyze, present, and act upon information to achieve specific mission duties. All information flows originate and terminate in applications via their (ideally embedded) transfer systems.

Mission Category. Applicable to information systems, the mission category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission. Mission categories are primarily used to determine requirements for availability and integrity services. DoD will have three mission categories:

a. Mission Critical. Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified information, as well as sensitive and unclassified information).

b. Mission Support. Systems handling information that is important to the support of deployed and contingency forces. The information must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

c. Administrative. Systems handling information, which is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified information, but is much more likely to be sensitive or unclassified information). (*DoD CIO Guidance 6-8510 IA*)

Mission Profiles. Expressions of general user needs in operational terms and may draw upon a broad range of information types from a number of producer sources.

National Security Systems (NSS). As defined in Clinger-Cohen Act 1996, NSS includes any telecommunications or information system operated by the United States Government, the function, operation or use of which involves intelligence activities; cryptologic activities related to National Security; involves the command and control of military forces; and involves equipment that is an integral part of a weapon system. Routine administrative and business applications are not included.

Near Real Time. Pertaining to the delay introduced, by automated data processing , between the occurrence of an event and the use of the processed data, *e.g.,* for display or feedback and control purposes. *Note 1:* For example, a near-real-time display depicts an event or situation as it existed at the current time less the processing time. *Note 2:* The distinction between near real time and real time is somewhat nebulous and must be

defined for the situation at hand. *Contrast with* **real time**. (2) Pertaining to the timeliness of data or information that has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP1)

Network. (1) An interconnection of three or more communicating entities. (2) An interconnection of usually passive electronic components that performs a specific function (which is usually limited in scope), *e.g.,* to simulate a transmission line or to perform a mathematical function such as integration or differentiation. *Note:* A network may be part of a larger circuit. (*MIL STD 188*)

Network Centric Warfare. An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

Network Management. The function of monitoring, controlling, and managing the provisioning of bearer (i.e., OSI layer 3 and below) services between two or more network elements that lie within a single common network. Network management is a sub-type of infrastructure management and is therefore a function that, while not part of IDM, must closely interact with the IDM organic functions.

Network Object. Any device, system, or application that connects to the GIG that a network manager controls. The network manager has visibility and maintains control over these objects for the Commander.

Network Operations. The organizations and procedures required to monitor, manage and control the GIG. Network operations incorporate network management, information dissemination management, and information assurance. (*DoD CIO Guidance 10-8460 NM*)

Node. In network topology, a terminal of any branch of a network or an interconnection common to two or more branches of a network. (*MIL STD 188*)
A network element that, while able to generate or receive a data stream across a network link, is not capable of providing an environment for the execution of an application. (See command node, IDM operational node, information distribution infrastructure node, producer node, user node.)

Non-repudiation. Provides the ability to prove to a third party that an entity did indeed participate in a communication. Non-repudiation is provided by the authenticating characteristics of digital signatures. (ASDIA)

Notification. The process of providing signals to Users of the immediate availability of data. By immediate, we mean that the data may be delivered to the User within some period of time that the User has previously specified. The type of signal must also have

been previously defined. Thus, notification services are driven, to a large extent, by a User interest profile. Notification services extend the services already available in the Web retrieval service to other information transactions such as delivery or system alerts from the metanet, transfer agent, and policy editor components.

On Demand. The user requests information based on their requirements and within the constraints of the commander's policy and the availability of the information. There are two methods for the user requesting the information. The first method is a user query for information based on the information producer's advertisement of the information availability. The second method is through the submission of a user-developed profile that requests that information be pushed on a regular user-defined schedule/preset frequency and/or pushed when available or as it has changed.

Open System. A system with characteristics that comply with specified, publicly maintained, readily available standards and that can, therefore, be connected to other systems that comply with these same standards. (T1 2000) One that consists of modular, multi-vendor, interoperable building blocks that are assembled into functional units.

Operational Suitability. The degree to which GIG components can be satisfactorily fielded, deployed, operated, and sustained while meeting performance parameters and the users' needs.

Planning Information. Planning information is used as a basis for determining future action and is generally not time sensitive. (JFCOM White Paper - C4 to Meet the Needs of 2010 and Beyond)

Policy Management. The function of overseeing the setting of, and access to, the commander's dissemination policies.

Policy Services. The aggregation of functions that support the commander and the user in the setting and usage of the commander's dissemination policy.

Prioritize. To establish a ranking system by precedence, usually to enable sharing of limited resources.

Producer. Information producers originate and supply information products in response to valid user/subscriber requirements.

Producer Node. Any node where a user participates in information processes, primarily as an information producer. A producer performs the following activities: (1) receives and responds to information profiles either directly through IDM tools or through his/her C4I mission applications; (2) generates information products and standard metadata descriptions of those products, often storing them in his/her C4I repository; (3) executes information transfers in response to on-demand requests or transfer or mission profiles; (4) responds to either on-demand or profiled information searches and catalog requests;

(5) monitors the IDM services to track the status of relevant activities; (6) specifies and manages information descriptor collections (catalogs).

Profile. Expression of information needs, interests, constraints, or requests (ad hoc or standing) by an information user, the user's designee, or their automated applications that enable filtering of information needed by specific users. This need is expressed independent of source but with emphasis upon timeliness required, thereby ensuring awareness of information requirements associated with mission/operation templates and consistent with applicable information policy. (1) A complete list of the information a unit must possess. (2) A detailed security description of the physical structure, equipment component, location, relationships, and general operating environments of an information system. (3) A set of parameters defining the way a device acts relative to other devices, including services required from others and provided by the device (often called a login file). (4) A profile or a combination of two types of information. First, the profile specifies a partitioning of the information space. What we mean by this is that the attributes of a metadata schema can be thought of as analogous to a geospatial coordinate system and a profile, by specifying values for these attributes (e.g., file size less the 2 Mbytes, format = JPEG), and defining regions within the information space. Any individual item of information may be located with respect to these regions (entirely inside, partially inside, entirely outside). Two key points to note are a) a single profile may specify multiple partitions (i.e., regions), and b) the "fineness" of the partitioning is limited to what may be specified by the metadata schema that is used (e.g., if the schema has the concept of nations and states but not counties, the profile will allow a distinction between information pertaining to people who live in California and those who do not, but will not allow a similar distinction between those who live in Orange County and those who do not). The second type of information contained within a profile is some sort of attribute that is to be associated with any information that falls wholly or partially within the specified partition. That attribute may be an indication of intent. By this we mean that for each partitioning specified, an indication must be provided as to what the entity associated with the profile wants to do or intends to do, with any information that falls within that partition (e.g., delete from the local cache, queue for later delivery, replicate to a set of repositories, notify the user upon receipt). Alternatively, the attribute specified in the profile may be one of description. For example, it might be a special security compartment or an indicator of frequency of access (e.g., a profile of all data accessed less than once per week).

Profiling. The process of defining automated information dissemination criteria. Identifies information certain users require according to a specific criterion, including restrictions of the producer on authorized recipients of the information.

Quality of Service (QoS) Forecast. A prediction of the quality of service that will be available to various communities of users. A QoS forecast may, for example, indicate that BDA imagery will be transferred to all intended recipients with a predicted latency of less than 30 seconds, that weather imagery will be transferred to in-theater recipients within 20 minutes and CONUS recipients within 30 minutes, and that medical data will have a predicted latency of 15 seconds for text data and 20 minutes for image data. The function of the QoS forecast is to provide a feedback mechanism that allows the

commanders to refine their policies and the operators to identify problems within the dissemination infrastructure.

Query. (1) A user request for additional or amplifying information regarding information received through some means. (2) In data communications, the process by which a master station (or mainframe or boss computer) asks a slave station to identify itself and tell its status (i.e., is it busy, alive, OK, waiting, etc.). (3) A data structure consisting of one or more search criteria and, associated with each search criteria, a set of actions. Search criteria are Boolean functions whose terms consist of metadata attributes (e.g., data of last modification, size), operators on those attributes (e.g., size <12000), or evaluation functions that operate on a data instance (e.g., key word found{China}). The set of actions associated with each search criteria indicates what the user wished to occur whenever the criteria evaluates to TRUE (e.g., retrieve the data instance, provide the user with a pointer to the data instance, provide the user with the metadata associated with the data instance, etc.).

Real Time. Pertaining to the timeliness of data or information, which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays.

Schema. Organizing structures for data; used in conjunction with a database management system or information product metadata management.

Search. To carefully and/or thoroughly peruse a domain for the purpose of finding or discovering something.

Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of information processed and stored by a computer or information system.

Security Services. The aggregation of those functions that support the creation and maintenance of information security policies and procedures.

Semantic Tag. Labeling of information based on the meaning of the content of the information and the context in which it appears.

Server. A network device that provides service to the network users by managing shared resources. *Note 1:* The term is often used in the context of a client-server architecture for a local area network (LAN). *Note 2:* Examples are a printer server and a file server (T1 2000). An information system component that provides client applications with access to a shared capability that the client does not directly support. It does so by responding to service requests from the client (it may also support service requests from other peer servers as well). A server may interact with other servers or functional entities as a result of a service request (e.g., a WWW proxy server redirects a browser's request to another server). (NOTE: A server is not to be confused with a computer that hosts functional entities implementing the server class.) The term “server” refers solely

to a function. Thus, there may be multiple computers implemented on a single server (i.e., CPU).

Smart Push. Transfer of information product(s) to information user(s) in response to profile(s) submitted (typically by the commander's staff) in anticipation of a group of information needs. (2) The process of creating a user profile of information requirements for continuous broadcast to an operating unit or supporting entity.

Spectrum Supportability. The assurance that the necessary frequencies and bandwidth are available to military systems in order to maintain effective interoperability in the operational electromagnetic environment. It includes spectrum certification, host nation coordination, frequency assignment, and electromagnetic compatibility.

Source. (1) Organization or other entity that produces information products and, possibly, their metadata. (2) The part of a telecommunication system that transmits information. (See information producer.)

Storage. The retention of data in any form, usually for the purpose of orderly retrieval and documentation. (*JP 1-02*)

Store. Provide space for and/or maintain custody of an item for purpose of its preservation and/or to enable its future use or orderly disposal.

Survival Information. Survival information requires immediate action such as to attack the enemy, avoid being attacked, and/or to prevent fratricide. It is, therefore, extremely time sensitive. (*JFCOM White Paper - C4 to Meet the Needs of 2010 and Beyond*)

Subscribe. Express a standing information request (profile).

System. The set of interrelated components consisting of mission, environment, and architecture as a whole that performs some coherent function or set of functions.

Theater Information Management. Integrated management of information within a Theater; expected to yield information flows more responsive to a CINC or similar command authority; expected specifically to integrate information management across J2, J3, J4, & J6 staff elements and functional communities.

Transfer. An activity involved in moving information from an initial location to one or more subsequent locations.

Transfer Agent. (1) An entity which interacts with source, communications, and user infrastructures to support the retrieval, transport, and delivery of information.(2) Any software module within a transfer system that supports information transfers in a manner that they may be managed by IDM services

Transfer Profile. A data structure governing the operation of a transferor.

Transport. Transport is the movement of information and/or knowledge among consumers, producers, and intermediate entities.

User. (1) Recipient of information products enabled by IDM services, governed by the recipient's profile and commander's policy. (2) A user is the ultimate consumer of all Data. (3) A user is a human (identified through a login process) authorized to use a system. Each human will map to one user, and each user map to one human. A user is unique across the system (IDM).

User Node. Where a user participates in information processes primarily as an information user. A user sets information, mission, and transfer profiles, performs information searches, requests source catalogs, requests information transfers on -demand, monitors IDM to track status of information requests, and specifies and manages information descriptors collections (catalogs) (*IDM CRD*)

User Profile. Information characterizing an information user, facilitating the efficient data distribution of appropriate information to the user. Examples of such end user information includes: allowed classification levels, user receive suite ID, times available, assigned subscriptions.

User Pull. Transfer of information product (s) to information user(s) in response to a request by and in a time frame defined by the user or their applications.

Visibility. Having the awareness of the status of a resource. It may or may not involve actually monitoring the resource. (*DoD CIO Guidance 10-8460 NM*)

Part III - Acronym List

ACRONYM	DEFINITION
ABIS	Advanced Battlespace Information System
ACTD	Advanced Concept Technology Demonstration
ALSA	Air, Land, Sea Application
AOR	area of responsibility
ASD	Assistant Secretary of Defense
AT&L	Acquisition, Technology and Logistics
ATM	Asynchronous Transfer Mode
BADD	Battlefield Awareness & Data Dissemination
BC2A	Bosnia Command & Control Augmentation
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C&C	Computing and Communications
CDP	commander's dissemination policy
CINC	Commander in Chief
CIO	Chief Information Officer
CJTF	Commander JTF
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
COCOM	Combatant Command
COE	Common Operating Environment
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOPS	concept of operations
COP	Common Operational Picture
COTS	commercial-off-the-shelf
CRD	Capstone Requirements Document
D&D	denial and deception
DEW	directed energy weapons
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DOS	denial of service
DRB	Defense Resources Board
DTG	date time group
EHF	Extremely High Frequency
EMP	Electromagnetic pulse

EP	Electronic protection
ES	Electronic Support
EW	electronic warfare
FIPS	Federal Information Processing Standards
FoAPS	Family of Applications, Processes, and Services
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GI&S	Geospatial Information and Services
GIG	Global Information Grid
GOTS	government-off-the-shelf
HGI	Human-GIG Interaction
HSI	Human Systems Integration
IA	Information Assurance
IBS	Integrated Broadcast Service
IC	Intelligence Community
ID	identification
IDM	Information Dissemination Management
IER	Information Exchange Requirement
IM	Information Management
IMO	Intelink Management Office
INFOSEC	Information security
IO	Information Operations
IPC	Interprocess Communications
IPT	Integrated Process Team
IS	Information Superiority
IT	Information Technology
ITW/AA	Integrated Tactical Warning and Attack Assessment
I&W	indications and warning
JITC	Joint Interoperability Test Command
JNMS	Joint Network Management System
JOA	Joint Operational Architecture
JROC	Joint Requirements Oversight Council
JTA	Joint Technical Architecture
JTF	Joint Task Force
JTRS	Joint Tactical Radio System
JTT	Joint Tactical Terminal
JV2010	Joint Vision 2010
KPP	Key Performance Parameter
MASINT	Measurements and Signature Intelligence
MILSATCOM	Military satellite communications
MLS	Multilevel Security
MNS	Mission Needs Statements
NAIC	National Air Intelligence Center
NATO	North Atlantic Treaty Organization
NBC	Nuclear Biological and Chemical
NIMA	National Imagery and Mapping Agency

NM	Network Management
NSS	National Security Systems
NTPC	Nuclear C2 Systems Technical Performance Criteria
OPCON	Operational Control
ORD	Operational Requirements Document
OSI	Open System Interconnection
QoS	quality of service
RF	radio frequency
SA	Situational Awareness
SABI	secret and below interoperability
SAR	Satellite Access Request
SATCOM	satellite communications
SCI	Sensitive Compartmented Information
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Network
S/NF	Secret/No Foreign
SSI	System to System Interface
STAR	Systems Threat Assessment Report
TACON	Tactical Control
TAMD	Theater Air and Missile Defense
TBD	To Be Determined
TCP/IP	Transmission Control Protocol/Internet Protocol
TED	Threat Environment Description
TTP	Tactics, Techniques, and Procedures
USD	Under Secretary of Defense
UTA	US Imagery and Geospatial Information Service Technical Architecture
WGS	World Geodetic Survey
WMD	Weapon of Mass Destruction
XML	Extensible Markup Language

Appendix B. Distribution List

To facilitate the widest possible access and distribution, the GIG CRD is posted on the World Wide Web at http://www.jfcom.mil/gigcrd.

Appendix C. Analysis Supporting Survival Information Dissemination KPP Timeliness Metric

The Joint Requirements Panel (JRP) has forwarded the Survival Information Dissemination KPP (with Threshold/Objective metrics) to the Joint Requirements Board (JRB) as part of the Joint Requirements Oversight Council (JROC) approval process.Analysis supporting the KPP timeliness metric can be found at the USJFCOM GIG CRD Website at http://www.jfcom.mil/gigcrd.

Appendix D GIG Information Exchange Requirements (IER) Matrix

GIG IER Matrix

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRI-TI-CAL	INFORMA-TION INTEGRITY	DATA ACCES-SIBILITY	Timeliness
SN 5 ST 5 OP 5 TA 5	Commander's Information Policy – Initial/Update	Policy	Command	IA,IDM,NM	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Request for information	Query	Command	IA,IDM,NM	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
			User	IDM				
			IDM	Producer				
			IDM	Store				
			Process	Store				
			IA,IDM,NM	IA,IDM,NM				
SN 5 ST 5 OP 5 TA 5	Response from Receiving Node	Results Of Query	IA,IDM,NM	Command	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
			IDM	User				
			Producer	IDM				
			Store	IDM				
			Store	Process				
			IA,IDM,NM	IA,IDM,NM				
SN 5 ST 5 OP 5 TA 5	Operational Assessment of IA, NM, IDM	Status	IA,IDM.NM	Command	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
	Operational Assessment of transport		Transport	NM				
	Operational Assessment		IA,IDM,NM	IA,IDM,NM				
SN 5 ST 5 OP 5 TA 5	Gain Access	Login/ Authentication	User	IA	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
			Producer	IA				
			Allies/C/Non	IA,IDM,NM				
SN 5 ST 5 OP 5 TA 5	Response to Login Request	Results of Login	IA	User	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
			IA	Producer				

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRI-TI-CAL	INFORMA-TION INTEGRITY	DATA ACCES-SIBILITY	Timeliness
			IA,IDM,N	Allies/C/Non				
SN 5 ST 5 OP 5 TA 5	Intrusion Fault	Detection Info	Transport Transport	IA NM	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Info to user as result of profile	Pushed info	IDM	User	Y	99.99% (T) 99.999% (O)	Semantic Tag*	Survival .05-2 sec Planning User-specified
SN 5 ST 5 OP 5 TA 5	Profile Approval	Authorized Profile	IDM	User	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Product Advertise-ment	Information Advertise-ment	Producer	IDM	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Request To Store	Storage Request	IDM	Process	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Provide initial configu-ration	Configu-ration	NM	Transport	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Change to Configu-ration	Network Changes	NM	Transport	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Respond to configu-ration changes	Acknow-ledge Changes	Transport	NM	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Provide Dissemin-ation Plan	Delivery Plan	IDM	NM	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Send	Input	Process User/ Producer	Process HGI	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Receive	Output	Process HGI	Process User/Producer	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Access	Authorization	Process	IA	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRI-TI-CAL	INFORMA-TION INTEGRITY	DATA ACCES-SIBILITY	Timeliness
SN 5 ST 5 OP 5 TA 5	Access	Results Of Authorization	IA	Process	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Store Data	Transactions	Process	Store	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Evoke Transport	Connection	Process	Transport	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Status On Connection	Feedback	Process	Transport	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Info Exchange	Transported Info	Process	Transport	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	End Info Exchange	Disconnect	Process	Transport	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified

Semantic Tag* - As Applicable

User-specified – The users' request for information based on their requirements and within the constraints of the commander's policy and the availability of the information. There are two methods for the user to request information. The first is a user query for information based on the information producer's advertisement of the information availability. The second method is through a profile that requests that information be automatically pushed on a defined schedule and/or pushed when available or as it has changed.